CERTS
CONSORTIUM FOR ELECTRIC RELIABILITY TECHNOLOGY SOLUTIONS

Integrated Security Analysis

Final Report

Project Team Members

Peter W. Sauer, University of Illinois at Urbana-Champaign

Kevin Tomsovic, Washington State University

Jeffrey Dagle, Pacific Northwest National Laboratory

Steven Widergren, Pacific Northwest National Laboratory

Tony Nguyen, Pacific Northwest National Laboratory

Lawrence Schienbein, Pacific Northwest National Laboratory

July 2004

Executive Summary

As economic pressures result in greatly expanded utilization of facilities, the issue of power system security analysis is key to reliable operation at maximum efficiency. Security analysis in this context refers to the ability of a power system to withstand pre-specified disturbances called contingencies. This report presents results on the identification of the current state of power system security analysis for operations and the potential integration of the various existing power system security analysis tools. Current security analysis consists of numerous software tools (some off-line and some on-line) that predict operator guidelines for transaction scheduling. A survey of selected operators in representative locations in both the East and Western US was conducted to determine the effectiveness of current tools and the need for future improvements. The primary outcome of that survey indicated that:

- There is a wide variation of satisfaction with the quality of the models used
- Network model reduction is done offline
- Virtually all operators are satisfied with their SCADA systems
- Virtually all operators have operational online power flow tools
- Most operators are satisfied with their state estimation tools
- Most operators are satisfied with their static contingency analysis tools
- Very few optimal power flow (OPF) tools are in use
- Almost no security constrained OPF tools are in use
- Some voltage analysis or dispatch is done off line
- Almost all transient stability analysis is done off line
- Virtually no midterm, long-term, or eigenvalue stability analysis is performed

This project also investigated alternative frameworks for the integration of existing tools into a comprehensive package that can be more responsive to changing conditions and simultaneous transactions. This portion of the project leveraged resources with a Power Systems Engineering Research Center (PSERC) project by the same title. These alternative frameworks build on the availability of raw data from existing security tools for both static and dynamic considerations as follows:

- On-line estimation of security margins using current operating practices
- Creation of families of estimators, each specialized for specific system limits
- Testing of estimators on simulated systems
- Automate the process of evaluating security margins in off-line studies

The results show that it is possible to accurately estimate security margins for large systems on-line. The main limitation of the approach resides in the ability of time-consuming off-line studies to accurately model system dynamics.

Table of Contents

1. Introduction

Power system analysis tools have existed in many forms since the 1920's [1]. By the 1950's the network analyzer was in wide use and digital simulation was being investigated. The formal introduction of the concept of security as a framework for planning and operating power systems emerged in 1967 [2]. The notion of the "normal state" being either "secure or insecure" depending on its condition after one or more hypothetical contingencies created the need to rapidly analyze the steady-state and dynamic behavior of a power system after a disturbance. In today's power marketplace, the ability to accurately and quickly determine system security limits has become even more a matter of economic importance as well as traditional reliability importance. Specific limits that must be checked for each contingency typically include:

- Thermal constraints on lines
- Voltage constraints at buses
- Margin to system voltage collapse
- Margin to system steady-state instability
- Margin to system transient instability

Over the past several decades, research has resulted in significant advances in analytical techniques needed for quantifying system security limits. At the same time, the phenomenal growth in computational speeds of modern computers has brought on-line security analysis closer to practical use. The first part of this project included a survey of operators at various organizations across the North American interconnected grid. The purpose of this survey was to:

- Inventory security analysis tools in use today
- Categorize the tools functions and robustness
- Evaluate the technical merits of the algorithms and their performance
- Identify gaps in tool capabilities and to address security issues
- Plan for Federal research and technology development to address the needs

A summary of the survey results is given in Chapter 2. The detailed results of this survey are included in Appendix A.

Early survey results quite clearly showed that there is a major gap in the operations security tools. This gap is the lack of an ability to evaluate stability margins in real time. The second part of this project focused on this gap and investigated the feasibility of a new technique for bringing dynamic analysis into the operations environment. The work started with two of the most time consuming aspects of stability margin analysis: time-domain simulation and static voltage margin computations. In a previous PSERC project [3], it was shown that a system of estimators based on Neural Networks could accurately and quickly estimate security margins for on-line application. That work considered only static voltage security and recommended *" … (investigating) other security criteria that may be less amenable to interpolation."* The approach in that project leads naturally to the more general framework proposed in this project. This framework is based on more sophisticated modeling and time-domain simulations.

In recent years, there have been several database or pattern matching methods introduced for finding security limits [e.g., 4-5]. The essential idea is to select a set of representative features (such as line flows, loads, and generator limits) and then train an estimator, (typically an Artificial Neural Network or ANN) on simulation data in order to estimate the security margin. The estimator is expected to interpolate or generalize to similar unstudied cases.

The problem with much of this previous work is that researchers have focused on generic power system models that ignore the practical difficulties in determining these limits and the specifics of reliability criteria for a particular system. Our earlier work has shown that accurate estimates can be obtained for voltage security on practical systems (in this case, the WECC system [6]) only by developing very narrowly focused estimators. For example, different ANNs can be trained based on certain major equipment outages and security criteria. In this project, this framework is extended to other security considerations. A hierarchical design is developed that combines margin estimators for different security criteria and operating conditions. A voting mechanism is introduced that combines individual estimates. Each estimator is designed using statistical criteria that ensure optimal performance [7]. The results show that it is definitely possible to very accurately estimate security margins for large systems on-line. The main limitation of the framework resides in the ability of time-consuming off-line studies to accurately model system dynamics. Directions for further development are proposed. The detailed results of this investigation are included in Chapters 3-7.

The advanced techniques proposed here have an important link to the issues expressed in the survey interviews. Several of the survey comments expressed a need to make dynamic security analysis operational in "real time" with minimal effort required of the operators. This was one of the main goals of the ANN approach.

2. Summary of Survey Results

This project included surveys of operators and operation planning engineers. The purpose of the surveys was to identify existing tools that are in frequent use as well as to identify any tool development needs that may exist in typical operations environments. The survey form that was prepared and used is included with the detailed results given in Appendix A. The names of the organizations surveyed are given in Table 2.1 below. In most cases only one person from each organization was interviewed. For this reason, not all of the information on the survey form was obtained from every organization.

Table 2.1 Organizations Surveyed

American Electric Power
American Transmission Company
Baltimore Gas & Electric
BC Hydro
Bonneville Power Administration
California Independent System Operator
Commonwealth Edison Company
Duke Energy
Florida Power Corporation
ISO New England
Kansas City Power and Light
Mid-American Interconnected Network
Northern States Power
Ontario Hydro Services
PJM Interconnection
Rocky Mountain Desert SW Security Center
Salt River Project
Southern Company Services
Southwest Power Pool

The primary security analysis tools in use are:

- Power flow program (linear and full AC) for thermal and voltage limit analysis
- Continuation power flow for voltage collapse analysis
- Eigenvalue analysis for determining steady-state instability margins
- Time domain analysis for determining transient stability margins

In almost all cases, the actual security "calculations" performed in the operations environment were focused on static security assessment only. All of the surveyed operators indicated that full AC load flow was the primary security analysis tool. Transient stability or voltage collapse issues were only evaluated when the full AC power flow indicated an unusual operating condition (such as questionable voltage profiles).

When voltage collapse or transient stability problems were suspected, the analysis was transferred to operations planners for detailed analysis. Some operators were guided by seasonal nomograms that were cataloged according to primary corridor loadings, or into “operator guidelines”. In several cases, operations personnel performed extensive time-domain simulations during day-ahead operations planning. In some cases this lack of dynamic security analysis activity was due to a lack of problems, or of interest in these phenomena. In other cases, it was due to a lack of efficient and integrated tools.

Of those operators that performed static security analysis only, there was an equal interest in finding voltage collapse and transient stability analysis tools. In many cases, the delay in finding these tools had to do with their low priority among other operational tasks, or high perceived overhead in getting the tools operational and maintaining new models. For those operators that were interested in future transient stability tools, there was a strongly-expressed concern that these tools should require operators to process a minimal amount of information. In one case, the operators expressed a need for a program that would systematically examine possible fault current levels after contingencies or planned outages to ensure that the protection system fault duties were adequate.

A detailed listing of specific survey responses is included in Appendix A.

3. New Security Analysis Tools

Power system security is the ability of a system to withstand sudden disturbances with minimum disruption to quality of service. Examples of such disturbances are electric short circuits, change of transmission system configurations due to faults, loss of system components, line-switching actions, and sudden load increases. For proper planning and operation, having a secure system means that after a disturbance occurs, the power system (1) will survive the ensuing transient and move into an acceptable steady-state condition, and (2) in this new steady-state condition, all components will operate within established limits [8]. The analysis used for the first requirement is transient analysis or Dynamic Security Assessment (DSA). The analysis for the second condition is static security assessment (SSA). In addition, voltage support has become an increasing concern so a third analysis is voltage security assessment (VSA), although this analysis often overlaps with SSA and DSA.

Typically, SSA is performed first, followed by DSA. SSA evaluates the post-contingent steady state of the system, neglecting the transient behavior and any other time-dependent variations. For on-line SSA, modern computational speeds allow load flow studies of a large number of contingencies in near real-time. Such software is a standard component of energy management systems (EMS), although this software usually does not directly compute security margins but simply evaluates static limits. Several other techniques are now available to quickly and reliably perform SSA, although they are not widely used in practice.

DSA evaluates the time-dependent transition from the pre-contingent to the post-contingent state determining the stability of the system for both small and large disturbances. Two dynamics problems, transient stability and voltage collapse, should be considered when performing a dynamic security study. Transient stability assessment is the major concern in DSA for multi-machine power systems analyzing whether a fault on the system, or loss of a large generator, can give rise to large electromechanical oscillations between generating units leading to a loss of synchronism in the system.

On-line DSA methods are still not fully operational, with some approaches currently being tested and evaluated. Research on on-line DSA has generally focused on using fast methods to quickly determine system stability, including both time-domain simulation for transient stability indices and various energy function methods. This is in sharp contrast to the comprehensive, detailed and time-consuming studies employed in operational planning. Conventional techniques for dynamic security analyses require excessive computational time. Therefore, these are generally undesirable for on-line purposes.

VSA has been based primarily on static or pseudo-dynamic methods, with some useful on-line tools available. The voltage stability problem is generally associated with the increased loading of long transmission lines and insufficient local reactive power supply. An initial gradual voltage drop, followed by a rapidly accelerating decline or collapse, characterizes these types of phenomena. The time interval of the slow voltage decay phase typically is between 1 to 10 minutes, which is often allows time for the operator to exercise corrective action.

3.1 Operations Planning and Reliability Policies

System security depends on the cooperation of different interconnected entities to coordinate operation of the system. The primary method to ensure this coordination in practice is to establish precise guidelines for the allowable effects neighboring systems may have upon each other. These guidelines are based on both field experience and extensive operational studies. Different performance levels are used, depending on the type of disturbance. For example, under WECC guidelines, allowable post-transient voltage deviation is 5% for a single generator outage and 10% for the outage of two generators. Thus, each reliability criteria depends on the type of disturbance. The disturbance should not violate constraints on:

- loading within emergency equipment ratings,
- transient voltage dip both in percentage deviation and in time duration,
- minimum transient frequency,
- post transient voltage deviation, and
- positive damping, i.e., stability.

Operation planners generally address these criteria through detailed time domain simulation studies for different loading conditions and for all major contingencies. In addition, there may be further requirements on running system studies. In the WECC, this includes using either the P-V method (MW margin) or V-Q method (MVar margin) to determine an adequate voltage security margin. System operators, to a greater or lesser degree depending on the utility, tend to rely heavily on the limits identified by operational planners and make relatively limited use of the on-line security tools.

Generally speaking, each operational planning study must look at static, dynamic and voltage security concerns. For a given loading condition and the status of any significant equipment out-of-service, response to all credible and major contingencies is investigated. The loading, or other key system parameter (KSP), is varied to determine the proximity, or margin, to a security problem. For example, in VSA, one employs P-V and/or V-Q curves [8] using the distance to the nose as the margin. The allowable margins and associated reliability criteria are based on the regional council guidelines [9]. Margins for each scenario can be determined and documented in look-up tables or nomograms. Nomograms graphically depict the system limits for some KSP given a few scenarios, such as scenarios involving equipment outages or large transfers. The operator will then base the real time decisions on this information.

Look-up tables have the obvious drawback of inflexibility and are prone to errors because operators must search for the relevant scenario in the tables. Nomograms, on the other hand, provide slightly greater flexibility as they depict trade-offs in operating conditions, such as between some loading condition and a transfer across a key interface. Still, nomograms fail to fully capture all the information contained in the off-line studies and lack the ability to manage more varied situations. This practical approach differs significantly from approaches described in much of the on-line security literature that focus on contingency screening and fast methods for calculating the security. In practice, security limits are tabulated off-line as described above.

3.1.1 Dynamic Security

In practice, the typical criteria for DSA include [10]:

- Inertial stability criteria. This mainly concerns the evolution of relative machine angles and frequencies.

- Voltage excursions (dip or rise) beyond specified threshold level and duration. This includes separate voltage excursion threshold/duration pairs for voltage dip and voltage rise, and maximum/minimum instantaneous excursion thresholds.

- Relay margin criteria. These are defined for pre-disturbance and post-disturbance conditions. If relay margin is violated for more than a maximum specified time after the disturbance, it is identified as insecure.

- Minimum damping criteria. For a designated list of contingencies, if the post-disturbance system exhibits oscillations, they must be positively damped (decreasing in amplitude).

Identifying the specific set of security constraints to be introduced for the dynamic security studies is based on experience, knowledge of the system, and judgment of the planning and operations engineers. Generally, the objective of DSA is to determine, which contingencies may cause power system limit violations or system instability. The ultimate goal is to generate the operating guidelines for defining the areas of secure operation. Generating the operating guidelines includes selecting contingencies, performing a detailed stability study, and analyzing the results for violations. Research on new methods for DSA can be divided into three areas: simulation (numerical integration method, direct or Lyapunov methods, and probabilistic), heuristic (expert system), and database or pattern matching approaches. An overview of these methods is provided below.

Numerical Integration

The numerical integration algorithms are used to solve the set of first order differential equations that describes the dynamics of a system model [11]. The most widely used methods are Runge-Kutta predictor and predictor-corrector methods. Numerical integration provides exact solutions relating to the stability of the system depending on the detail of the models employed. This is most widely applied approach in off-line environments, but is generally too computationally intensive for on-line application.

Direct/Lyapunov Methods

This approach is also referred to as the transient energy function (TEF) methods. The idea is to replace the numerical integration by stability criteria. The value of suitably designed Lyapunov function V is calculated at the instant of the last switching in the system and compared to a previously determined critical value V_{cr} . If V is smaller than V_{cr}, the post-fault transient process is stable [12].

In practice, there are still some unresolved problems and drawbacks of this approach.

- The efficiency of this method depends on simplification of the system variables.
- The integration of the fault-on system equations is needed to obtain the critical value for assessing stability.
- It is difficult to construct the appropriate Lyapunov function to reflect the internal characteristics of the system.
- The method is rigorous only when the operating point is within the estimated stability region.

Probabilistic Methods

With these methods, stability analysis is viewed as a probabilistic rather than a deterministic problem because the disturbance factors (type and location of the fault) and the condition of the system (loading and configuration) are probabilistic in nature. Therefore, this method attempts to determine the probability distributions for power system stability. It assesses the probability that the system remains stable should the specified disturbance occur. A large number of faults are considered at different locations and with different clearing schemes. In order to have statistically meaningful results, a large amount of computation time is required [13]. Therefore, this method is more appropriate for planning. Combined with pattern recognition techniques, it may be of value for on-line application.

Expert System Methods

In this approach, the expert knowledge is encoded in a rule-based program. An expert system is composed of two parts: a knowledge base and a set of inference rules. Typically, the expertise for the knowledge base is derived from operators with extensive experience on a particular system. Still, information obtained off-line from stability analyses could be used to supplement this knowledge. The primary advantage of this approach is that it reflects the actual operation of power systems, which is largely heuristic based on experience. The obvious drawback is that it has become increasingly difficult to understand the limits of systems under today’s market conditions characterized by historically high numbers of transactions.

Database or Pattern Recognition Methods
The goal of these methods is to establish a functional relationship between the selected features and the location of system state relative to the boundary of the region of stability [14,15]. This method uses two stages to classify the system security: 1) feature extraction and 2) classification. The first stage includes off-line generation of a training set of stable and unstable operation states, and a space transformation process that reduces the high dimensionality of the initial system description. The second stage is the determination of the classifier function (decision rule) using training set of labeled patterns. This function is used to classify the actual operating state for a given contingency. Typically, the classifier part of this approach is implemented using ANNs.

3.1.2 Voltage Security

Voltage stability margin is a measure of the available transfer capacity, net transfer capacity, or total transfer capacity. The margin is the difference (or a ratio) between operation and voltage collapse points based on the KSP (loading, line flow, etc.) and accounts for a pattern of load increase or generation loss. As a concept for system operators, margin is a straightforward and easily understood index, and thus, widely accepted. There are a number of advantages of the stability margin as a collapse index.

- The margin is not based on a particular power system model and can be used with static or dynamic models independent of the details of the power system dynamics.
- It is an accurate index that takes full account of the power system non-linearity and device limits as loading is increased.
- Sensitivity analysis may be applied easily and quickly to study the effects of power system parameters and controls.
- The margin accounts for patterns of load increase.

The primary disadvantage is that it may oversimplify the view of the stability problem and may not account for the variety of ways in which instabilities can arise.

In theory, the computation of the stability margin should be performed for all contingencies. This would be an excessively time-consuming process but is generally not necessary in practice. Instead, the margin is determined based on the most critical contingency from a relatively short list of known severe contingencies. Key to the analysis is the degree of experience that allows one to identify a more manageable list of disturbances. Still, the precise computation of the margin is time-consuming, thus limiting application for on-line use.

The most common methods to estimate the proximity of the voltage collapse point are the minimum singular value, point of collapse method, continuation power flow, and optimization methods. Some other methods are sensitivity analysis, second order performance index, and the energy function method.

The minimum singular value of load-flow Jacobian matrix has been proposed as an index for quantifying proximity to the voltage collapse point [16]. It is an indicator easily available from normal load-flow calculations. The method is based on the analysis of a linear system. The singular value decomposition is applied to the linearized load-flow equations to analyze power system voltage stability. The analysis studies the influence of a small change in the active and reactive power injections to the change of angle and voltage. A Jacobian matrix is a linearisation at the operation point and the voltage stability problem is non-linear in nature. If the operation point is far away from the voltage collapse point, then the minimum singular value does not describe the state of the system accurately. The minimum singular value of a load-flow Jacobian matrix is also sensitive to the limitations of generator reactive power, transformer tap changer and compensation device.

The point of collapse method is a direct method [17]. It computes the voltage collapse point, the power demand, and corresponding state variables directly without computing intermediate load-flow solutions. The method is based on bifurcation theory and the singularity of the load-flow Jacobian matrix. In applying bifurcation theory to power systems, the power demand is often used as the slowly changing parameter. A voltage collapse point is found by changing the parameter in a specified direction.

The purpose of the continuation load-flow is to find a continuum of load-flow solutions for a given load/generation change scenario (or computation direction) [18]. It is capable of generating the full PV curve. The continuation load-flow finds the solution path of a set of load-flow equations that are reformulated to include a continuation parameter. This scalar equation represents phase conditions that guarantee the non-singularity of the set of equations. The method is based on prediction-correction techniques. Another direct computation method of voltage collapse point is the optimization method [19] In this approach, the voltage stability margin is maximized according to the load flow equations and power system constraints. Generally, the optimization is not global over the parameter space.

3.1.3 Remarks

To bridge the gap between the practical procedures employed to determine power system interface limits and the various proposed methods for on-line security, requires consideration of a number of factors.

- Operational planning methods cannot identify all possible operating conditions that may arise and are generally too slow to repeat on-line when unstudied system conditions arise.
- Operators do not have full access to all the detailed assumptions that might have been used in an off-line study. Furthermore, they only have access to the

conclusions of a study (i.e., the actual transfer limit and limiting outage) and not all the underlying case studies that might have been performed.

- Many of the proposed on-line security methods are fast methods to determine security, but are not as effective at determining a practical operating limit, such as the transfer between systems.
- The various proposed on-line security methods work well under certain conditions but will fail at other times in ways that may not be well-understood.
- Most of the on-line security methods do not base assessment on the detailed reliability requirements employed by the various regional councils.
- Practical system security assessment always has a certain degree of system specific considerations that do not lend themselves to more formal analysis.
- Most operators are not well versed in the computational techniques employed in security analysis and hesitant to place confidence in “black box” approaches.

3.2 WECC Reliability Criteria

The reliability councils in the U.S. have criteria that must be satisfied by entities that operate in their geographical region. These criteria are typically identified in formal contracts that are executed between the entities and the councils. This section provides a discussion of the WECC reliability criteria to establish a typical environment for operations. Continuity of service to loads is the primary objective of the reliability criteria. Preservation of interconnected operation during a disturbance is secondary to the primary requirement of preservation of service to loads. Although allowing for the possibility of failures, each system within the WECC must strive to protect its customers against loss of service. The reliability criteria may be defined and measured in terms of the performance of a system under conditions of stress. Prediction of performance requires extensive simulation because actual tests on existing systems are not practical.

3.2.1 Performance Levels

The reliability councils specify different performance levels based on the severity of a disturbance. The minimum allowable performance levels for interconnected bulk power systems range between having no appreciable adverse system effects to having substantial effects, perhaps involving load shedding and controlled islanding. The minimum level of performance that is acceptable under simulation tests is presented in Table 3.1, referred to as the “Disturbance-Performance Table.” This table defines the performance to be expected for a given class of initiating disturbances. A higher level of performance is required for disturbances that generally occur with a higher frequency or likelihood.

Types of elements lost due to various disturbances are listed in the Disturbance-Performance Table in descending order of frequency and increasing order of severity. Performance is specified as five discrete levels: A, B, C, D and E. Levels A through D do not permit any uncontrolled loss of generation, load, or uncontrolled separation of transmission facilities. For Level E disturbances, uncontrolled loss or separation may occur. Within Level E, a number of extreme contingencies that are judged to be critical by the transmission planning entity are selected for evaluation. Initiating events must be viewed as being associated with a specified performance level.

The Disturbance-Performance Table portrays these ranges by giving several examples of disturbances considered under each category; however, it is not exhaustive. Only a limited number of all possible facility outages under each listed contingency are evaluated. The examples presented should provide a basis for estimating performance levels for disturbances that are not listed. When multiple elements are specified, they are assumed to be lost simultaneously. In cases where a prior outage exists on a system, system adjustments will be made to allow the system to meet the required performance specified for the next disturbance. As an example, the loss of a generator with a prior system condition of one generator out is not considered a simultaneous loss of two generators. The table applies equally to either of the following: (a) a system with all elements in service; or (b) a system with one element removed and system adjustments made following the outage.

The different levels are summarized here below with details given in Table 3.1 [9].

- Level A performance should produce no significant adverse effects outside of the system in which the disturbance occurs. This includes loss of load (firm or interruptible) or facility loadings that are outside emergency limits.
- Level B performance allows for some adverse effects that may occur outside of the system in which the disturbance occurs. For example, interruptible load shedding may occur, but there should be no loss of firm load. Facility loadings should remain within emergency limits.
- Level C performance allows substantial adverse effects outside of the system in which the disturbance occurs. Firm and interruptible load shedding may occur, but facility loadings should remain within emergency limits.
- Level D performance seeks only to prevent cascading and the subsequent blackout of islanded areas. Some additional adverse affects may occur, including firm and interruptible load shedding or sustained (but not growing) oscillations.
- Level E performance seeks only to evaluate risks and consequences. Additional adverse system impacts that may occur are substantial loss of customer demand and generation in a widespread area or areas. Portions or all of the interconnected systems may or may not achieve a new, stable operating point.

Table 3.1 WECC Disturbance-Performance Table of Allowable Effects on Other Systems [9]

Performance Level	**Disturbance:** **- No fault** **- 3-phase fault with normal clearing** **- Single line to ground fault with delayed clearing** **- DC Disturbance**	**Transient Voltage Dip Criteria**	**Minimum Transient Frequency**	**Post Transient Voltage Deviation**	**Loading Within Emergency Ratings**	**Damp-ing**
A	Generator One Circuit One Transformer DC Monopole	Max *V* Dip - 25% Max Duration of *V* Dip Exceeding 20% - 20 Cycles	59.6 Hz Duration of *f* Below 59.6 Hz – 6 cycles	5%	Yes	>0
B	Bus Section	Max *V* Dip - 30% Max Duration of V Dip Exceeding 20% - 20 Cycles	59.4 Hz Duration of *f* Below 59.4 Hz – 6 cycles	5%	Yes	>0
C	Two Generators Two Circuits DC Bipole	Max *V* Dip - 30% Max Duration of *V* Dip Exceeding 20% - 40 Cycles	59.0 Hz Duration of *f* Below 59.0 Hz – 6 cycles	10%	Yes	>0
D	Three or more circuits on common ROW			Cascading Is Not Permitted		
E	Loss of multiple 500 kV or higher circuits (3 or more) that cross one another at 1 location Loss of 3 or more circuits that share a common linkage Loss of entire plant with 3 or more generating units Loss of entire substation Loss of multiple circuits, multiple generators, or circuits and generators that have no common mode of failure			Evaluate for risks and consequences		

3.2.2 WECC Voltage Stability Criteria

It is well-known that voltage magnitudes alone are poor indicators of voltage stability or security. Voltages can be near normal with generators, synchronous condensers, and SVCs near current limiting levels, thus resulting in a possible voltage collapse. Therefore, it is prudent to specify a MVar margin or MW margin. In the WECC, voltage stability criteria are expected to apply equally to studies of interfaces and load areas. Interfaces include major WECC paths, tie lines with neighboring systems, and critical paths within a system. The WECC voltage stability criteria are specified in terms of real and reactive power margins. The margin for *N-0* (base case) conditions must be greater than the margin for Performance Level A to allow for unforeseen increases in load or interface flows without remedial action schemes that would be activated during contingency conditions but not during normal conditions.

Table 3.2 lists the voltage stability criteria and the minimum margins for each disturbance level. Again, these apply equally to the system with all elements in service as well as the system with one element removed, and follow the general philosophy that a higher level of performance is required for disturbances generally having a higher frequency of occurrence. The system elements include any facility, such as generator, transmission line, transformer, and reactive power source. The determination of credibility for contingencies is based on the definitions used in the WECC Reliability Criteria [9]. The contingencies to be studied include the outage of any system elements which would impact the required margins. When multiple elements are specified, they are assumed to be lost simultaneously. In cases where a prior outage exists, system adjustments should be made to allow the system to meet the required performance specified for the next disturbance. As an example, the loss of a generator with a prior system condition of one generator out is, as indicated above, not considered a simultaneous loss of two generators. This is because the system should be re-dispatched, or other corrective actions should be initiated following the outage of the first generator.

From Table 3.2, the performance level A margin requirement is 5%, decreasing by one-half for subsequent performance levels. The 5% quantity refers to the KSP for a given study. Thus, if the study considers a transfer across a key interface, then it is 5% of that flow that establishes the required margin. These numbers are subject to re-evaluation by the WECC, but they are generally representative of current practices.

Table 3.2 WECC Voltage Stability Criteria [20]

Performance Level	**Disturbance:** **- Fault or No Fault** **- DC Disturbance**	**MW Margin**	**MVAR Margin**
A	Any element such as: One Generator One Circuit One Transformer One reactive Power Source One DC Monopole	≥ 5%	Worst Case Scenario
B	Bus Section	≥ 2.5%	50% of Margin Requirement in Level A
C	Any combination of two elements such as: A Line and a Generator A Line and a Reactive Power Source Two Generators Two Circuits Two Transformers Two Reactive Power Sources DC Bipole	≥ 2.5%	50% of Margin Requirement in Level A
D	Any combination of three or more elements such as: Three or More Circuits on ROW Entire Substation Entire Plant Including Switchyard	> 0	> 0

3.3 Estimation of Stability Margins

The previous discussion establishes the need for fast and accurate tools to evaluate security. For on-line application, a pattern matching or interpolation method rather than analytic approaches may be most appropriate. Among the alternative methods, artificial neural networks (ANNs) is the most promising [21] because ANNs have excellent generalization capabilities, superior noise rejection, and fast execution (with most of the calculations occurring during the initial off-line training).

Over the past decade, a number of approaches using artificial neural networks have been proposed as alternative methods for DSA in power system operations. Sobajic and Pao proposed a technique using a multi-layered network to predict the critical clearing time (CCT) for a given system disturbance [22]. In their paper, the authors showed that the neural networks generalize to previously unencountered system topologies and load levels, and correctly estimate CCTs. In a follow-up paper, they presented a combined unsupervised and supervised learning algorithm to solve the same problem [23]. The input data were pre-processed using an unsupervised learning system to enhance the accuracy of the supervised learning algorithm.

El-Sharkawi et al exploited a multi-layer perceptron to predict the dynamic stability status of a power system [24]. A layered perceptron was trained to learn the mapping between varying system operating state, active and reactive power injections in some system buses and the corresponding dynamic security status. Kumar et al [25] discussed implementing a neutral network for DSA in a large system, and proposed a hybrid expert system/neural network approach. The hybrid approach uses the knowledge of system operators in training neural networks. Mansour et al [26] proposed a neuron network approach to provide contingency screening and ranking in dynamic security. The B.C. Hydro and Hydro-Quebec systems were used to test the neuron network. The static and dynamic features were used as inputs, and the selected outputs were energy margin and maximum swing angle. In our previous work [6], an ANN was applied to estimate Q-V margins in the WECC system.

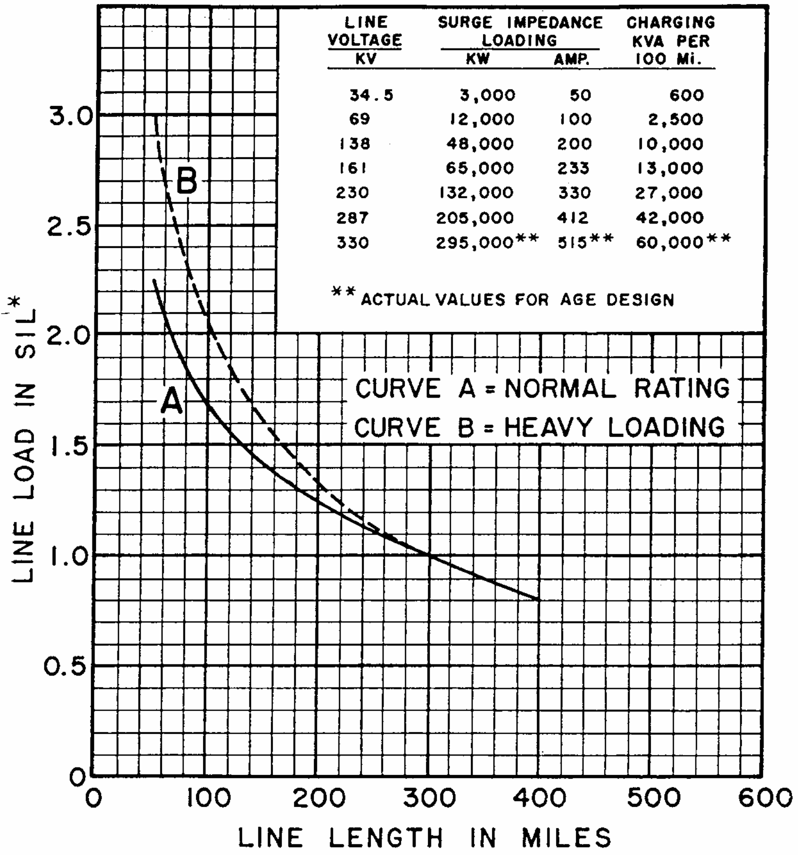
The primary limitation of the above approaches has been their failure to fully employ the system specific studies used in practice. This project addresses that limitation by using the exact WECC reliability criteria in the system security studies.

Security analysis is done, to some degree, to support planning and operations functions. In the planning function, time is not critical and extensive security studies can be performed without the performance constraints of analyses done to support operations. However, in the planning function, the base case condition is not known with certainty. While there is some uncertainty associated with establishing the base case in operations analyses, there is generally much less uncertainty about topology and state values. The primary need for security analysis is critical in meeting operations functions. However, combined security analysis concepts discussed in this section are also valuable for planning functions.

3.4 Combined Security Analysis Concepts

This project's primary focus is on developing a method that can systematically combine the results of different types of security analysis into one comprehensive framework. One objective of this focus is to avoid overlap of repeated computational algorithms. This overlap can be avoided if capabilities or margins can be computed for classes of designs or conditions that are independent of time and of load distribution. An existing example of this independence, in a basic form, is the "St. Clair" curve [27] that addresses six basic factors limiting the capability of a transmission line - voltage level, stability, line current, net reactive loss, resistance loss, and actual temperature rise. When used to compute the permissible loading for lines of various lengths, the limiting factors can be compressed into a single curve giving line loadability in SIL (Surge Impedance Load) vs. line length, as shown in Fig. 3.1 below.

This original St. Clair curve was the motivation for an analytical formulation of line limits of higher voltages and longer lines [28]. The analytical model used a pi section for the transmission line, with sending-end and receiving-end equivalent lines and sources. This simple equivalent was then used to evaluate the loadability with the criteria of thermal rating, voltage drop, and steady-state stability margin (based on the angle across the system). This analytical model allows the reproduction of the existing St. Clair curves as well as their extension to other voltage levels, line lengths, and system parameters. The conclusion was that lines are thermally limited when they are less than 50 miles long. In addition, between 50 and 190 miles, the loading is limited due to the voltage drop across the line. Finally, for lines longer than 190 miles, the loading is limited due to the margin to steady-state stability across the system. Caution in generalizing these conclusions was expressed in [29] because the reactive power supply capability was shown to be a critical parameter in allowing the stability margin portion of the St. Clair curves to be correct.



LINE VOLTAGE	SURGE IMPEDANCE LOADING		CHARGING KVA PER
KV	KW	AMP.	100 Mi.
34.5	3,000	50	600
69	12,000	100	2,500
138	48,000	200	10,000
161	65,000	233	13,000
230	132,000	330	27,000
287	205,000	412	42,000
330	295,000**	515**	60,000**

** ACTUAL VALUES FOR AGE DESIGN

Fig. 3.1. St. Clair curve

Most recently, the difference between MVA and MW limits on lines was examined in relation to power transfer capabilities. Techniques to convert between these limits, and other issues associated with reactive power considerations, are described in detail in [30].

While knowing the constraints on lines and corridors is an important part of security analysis and dispatch, knowing how to change the constraints is also important. Translating individual constraints due to thermal, voltage, and stability limitations into a line flow (MW) limit hides the actual cause of the constraint. In addition, the line flow limit does not indicate how the constraints might be relaxed by operator actions, or by addition of new facilities or components. For example, if the true constraint is a voltage drop limit, the possible methods to increase the constraint might involve reactive power siting, such as of new capacitors or other reactive power sources. These remedial designs could indeed increase the line flow (MW) limit more directly and more economically than upgrading the line capacity through construction of parallel lines. Thus the integration of security analysis tools must be done carefully and with the understanding that all options should be considered to provide meaningful results for security enhancement.

An additional approach to integrating security analysis involves prioritizing the various security analysis tools and the phenomena that they are designed to capture. For example, it should not be necessary to perform steady-state or voltage stability analysis to simply determine the stability of a post-contingency condition if time domain simulation is used to assess transient stability. As a matter of contingency screening, the integrated security analysis should use fast computational methods to determine insecure contingencies. In other words, if a contingency results in a simple-to-compute thermal overload, then there is no need to conduct more difficult analyses of voltage or stability insecurities. This indicates that the integrated analysis should start with phenomena that are easy to compute, and then proceed to more difficult analysis only if all contingencies pass the simple tests.

Just as the St. Clair curves have successfully integrated several security constraints in a single quantity, there is a need to extend this concept to more security analysis programs.

This portion of the project seeks to provide a comprehensive integration of existing security analysis programs into a new security tool suitable for the operations environment. This is done by focusing on the dynamic security analysis challenge together with the voltage collapse analysis challenge. These two were chosen because they remain the most difficult security analysis computations, and currently the least commonly used tools.

4. Proposed Methodology

In this section, a framework is introduced to integrate the various security assessment methods outlined above and to take advantage of the benefits of using pattern matching approaches. Power system security assessment can be divided into two categories: classification and security limit determination. Classification includes determining whether the system is secure or insecure under all pre-specified contingencies. Classification does not indicate the distance from the base operating condition to the insecure conditions. Security limit determination, on the other hand, involves finding this distance. Safe operating levels based on various system conditions are given in terms of the KSP (e. g., loading of a certain power plant, the power flow at a critical transmission interface, and the voltage at given bus).

The reliability standards require that the system be operated with sufficient margins to withstand any single contingency without experiencing overloads, low voltages, sustained oscillations or excessive frequency dip. For most utilities, the margin for each study case is used to produce a nomogram. Typically, the nomogram has a two-dimensional graph with the two axes corresponding to two critical parameters. All other critical parameters are set to selected values within a typical operating range.

In our framework, the power system security limit, in response to all predefined contingencies, is investigated for a given pre-contingency steady state of the system. The loading is varied to determine the security margin relative to each of the reliability criteria. The allowable margins and associated reliability criteria are those outlined above based on WECC guidelines for performance level A [9].

4.1 Overall Security Framework

The primary method to take better advantage of the off-line operational studies is to form a type of associative memory. In each of the study case, system conditions and the estimated security margin are. There are several conclusions from our analyses using this approach.

- Simple linear regression models cannot accurately estimate security margins.
- Feedforward ANNs have the best understood design criteria and, for this type of estimation problem, display the most favorable performance.
- No single estimator appears to be workable across a variety of security indices or widely different network topologies regardless of the number of study cases.

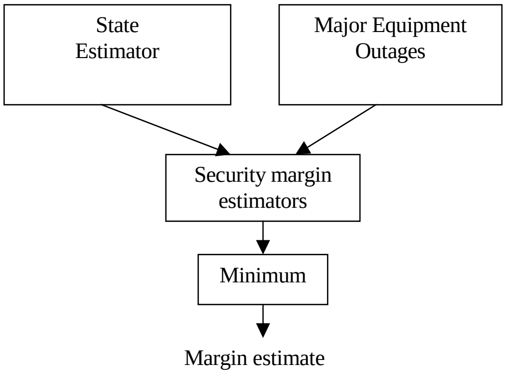


Fig. 4.1 Overall security margin estimation

- A family of smaller ANNs with different network parameters whose estimates are combined through a voting mechanism will perform better than a single large ANN.

As a result of our findings, we use several layers to the on-line estimation of security limits. At the highest level, the current state and major equipment outages are used to identify the appropriate set of margin estimators. This is depicted in Fig. 4.1. At this point in the development of the integrated security analysis framework, the minimum of all the estimated security margins are used because we have full confidence in the detailed models used to calculate the margins. However, a conceivable extension would be to allow for approximations, where the estimator is estimating a less precise margin. That approach is not investigated in this project to avoid ambiguities in the findings that may arise due to use of some particular index.

The set of estimators includes different estimators for different topologies. This does not imply a separate estimator for each outage scenario. For example, one estimator may represent (1) the base case, (2) a wide range of operating conditions, and (3) one or two major equipment outages. Another estimator could represent a similar set of operating conditions, except for different major equipment outages. This is in addition to the fact that the calculated margin is based on all chosen contingencies. As a result, each estimator could represent several nomograms. This is emphasized graphically in Fig. 4.2.

At the lowest level, a family of ANNs is used to estimate the security margin for a specific security criterion and operating condition. Fig. 4.3 shows the structure of an estimator for a given set of operating conditions and a specific security criterion.

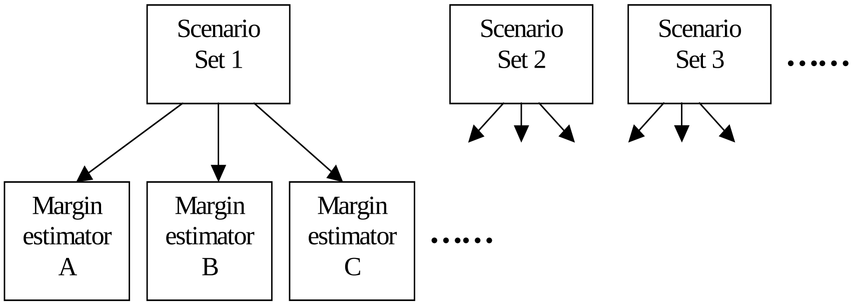


Fig. 4.2 Hierarchical structure of security margin estimators

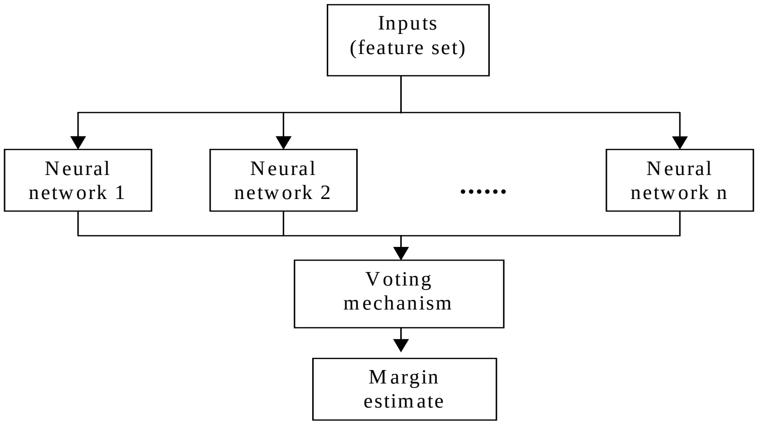


Fig. 4.3 Individual estimators with voting mechanism

4.2 Generation of Training Data

To determine the transient stability transfer limits or loading margins, a load flow must first be executed to insure that a given topology provides a satisfactory steady-state case. This steady-state case is then applied to initialize the network for the transient-stability simulation program. The program we use is the Extended Transient/Midterm Stability Program (ETMSP). When the simulation is completed, reliability criteria are applied to the extracted results from ETMSP. If the performance is adequate, then the loading is incremented and the load-flow software inputs are modified accordingly. This is repeated until the highest acceptable transfer level for an interface is found.

In general, to find the security limit, the process must be repeated for different contingency types and locations until the most constraining (i.e., lowest) transfer limit has been identified. It is impossible to pre-study all possible contingencies because the assessment processes are very time-consuming, and the analysis of every degraded topology is a problem of combinatorial dimensions.

For each of the system performance criteria identified in Section 3.2, the limits of the power system operation are established. These limits may be total load in an area, interface transfer limit, or some other KSP. Starting from a base case, the set of relevant system variables is recorded and a full analysis of all major contingencies is performed. The KSP is incremented and the analysis repeated until the system limits are identified. Thus, for each performance criterion, there is a large set of studies that establish the operating limit and a correspondingly large set of variables describing the operating conditions.

There are three software packages used in the studies.

IPFLOW [31]
IPFLOW is interactive power flow software developed by EPRI. For the dynamics studies, it provides the initialization before any disturbances are considered.

VSTAB [32]
The VSTAB (Voltage STABility) program, developed by Ontario-Hydro with EPRI support, is a voltage stability assessment package for large complex power systems. It provides information on the proximity to and mechanisms of voltage instability. VSTAB uses a power flow(i.e., a steady state technique) for voltage “stability” analysis.

ETMSP [33]
The ETMSP (Extended Transient/Midterm Stability Program) package developed by Ontario-Hydro with EPRI support. It is used to analyze power system dynamics following disturbances.

4.3 Estimator Design

The simplest form of an estimator is a simple linear regression model. We assume that the relationship between system variables and the margin can be modeled by a linear combination of first and second order terms. We write:

$$Y = \beta_0 + \beta_{11} X_1 + \beta_{12} X_1^2 \cdots + \beta_{1n} X_n + \beta_{n2} X_n^2 + \mathbf{e} = X\boldsymbol{\beta} + \mathbf{e} \qquad (1)$$

where Y is the observation (for us, the security margin) and X is the input feature set (e.g., line flows). The maximum likelihood (or unweighted least-squares) estimate of the parameters $\boldsymbol{\beta}$ is simply:

$$\hat{\boldsymbol{\beta}} = (X^{\mathrm{T}} X)^{-1} X^{\mathrm{T}} Y \qquad (2)$$

Of course, there are number of variations that can be introduced in this basic model. However, as will be seen, the non-linearities of the security analysis problem generally render the linear model approach problematic. The basic linear regression model is introduced to show the difficulty of simple interpolation. The estimators proposed in this work are feedforward ANNs based on the Levenberg-Marquardt and Bayesian Regulation algorithms [7]. Primary considerations in design of the neural network are outlined in the following section.

4.3.1 Feature Selection and Processing

Selected features should be based on engineering knowledge and statistical correlation between the selected features and the margins computed from security studies. These features will typically be variables such as real and reactive power flow, reactive power reserve, and voltage levels. A large set of features can be selected and then carefully reduced based on correlation coefficients.

This stage is an extremely important pre-processing step, as selected features must characterize properly a variety of power system operating conditions. Generally, the dimension of the pattern vector is very large. Feature selection is the process of finding the most significant variables, eliminating redundancy and reducing the dimension of the pattern vector. A number of different methods, most based on statistical approaches, are available for feature extraction (i.e., reducing the dimension of the input data vector). The parameters that may be applied to describe a system state are:

- The voltage magnitude and phase angle at each system bus
- The active and reactive power of each bus load
- The active and reactive power flow of all the lines
- The active and reactive power output of each generator plant.

The selection and extraction process involves engineering judgment and statistical analysis. The statistical analysis uses correlation coefficients and principal components analysis. The correlation coefficients between the selected features and the computed security margin are determined first. Subsequently, principal components analysis can be used. Principal component analysis (PCA), also called Karhunen-Loeve expansion, assesses the independence of the features in the selected feature set [7]. The PCA method determines the eigenvectors corresponding to the largest eigenvalues of the auto-correlation matrix of training vectors as its principal components. The reduced training vectors are selected in the direction of the most dominant eigenvectors. In essence, an orthogonal set of features is sought to present to the estimator, improving both training time and accuracy. For example, for the P-V margin estimator for the WECC system [6], the 106 system variables were reduced to 46 for training. The ANN is then trained with this new set of reduced vectors. This extraction closely relates to the performance of a neural network and computation time because the fewer the number of features, the fewer are the number of required samples..

4.3.2 Network Structure, Hidden Layers and Voting Schemes

Generally, multiple hidden layers improve the approximation process. Two hidden layers are needed when finding estimates for larger systems with more complicated non-linearities. The number of nodes in the hidden layers significantly impacts the performance. In the Bayesian framework of MacKay [34], the parameters are estimated using statistical techniques. several ANNs with parameters near the calculated optima are trained. The estimates from these networks can be combined using a voting scheme. For example, one effective method is to disregard the lowest and largest margin estimates from such a set of networks and then average the remaining estimates.

4.3.3 Splitting Training Data for Estimation and Validation

A statistical theory of the overfitting phenomenon that may occur with ANNs is presented in [35]. If N is the size of the training set and W is the number of free parameters in the network, with $N<W$, the optimum split of the training data between estimation and validation subsets is given by

$$r_{opt} = 1 - \frac{\sqrt{2W-1}-1}{2(W-1)} \tag{3}$$

where is r_{opt} is the fraction to be used for training.

5. Numerical Results

This section presents detailed analysis of the proposed methodology applied to (1) a small test system, a modified IEEE 39 bus system, and (2) a large practical system, a model of around 6000 buses of the WECC system.

5.1 Studies on IEEE 39 Bus System

5.1.1 System and Case Study Description

To illustrate the proposed approach, the New England 39 bus system is chosen. The system is divided into two zones, one load center of only the load buses 17, 18, and 27 with three tie lines 3-18, 16-17, and 26-27, as shown in Fig. 5.1. The other zone contains all other load and generation buses. The focus of study is the power flow at the interface of this load center. The study applies only on the WECC disturbance criteria for performance level A [9] considering only three phase faults with normal clearing.

The security margin is calculated by increasing the active power of the load center incrementally over the base case until there is a violation of the reliability criteria. The total system loading for the base case is 6150.5 MW and 1658.90 MVar. The flow across the interface of this load center is the parameter of interest. The entire data set consists of 983 samples, 20% for testing and 30% for validation. The training and testing data are obtained from transient stability studies using IPFLOW and ETMSP. Contingencies considered are three-phase faults on each line. For each load level, there are 31 cases, representing one base case and the 30 (n-1) contingencies.

5.1.2 Analysis

The first performance criteria considered is voltage stability as seen by the post-disturbance voltage response. The maximum voltage dip at any bus following a contingency cannot exceed 25% and a more than 20% dip cannot last for more than 20 cycles. The post-transient voltage dip should not exceed 5%. Finally, there must be positive damping. At times, these criteria will overlap with the dynamic security criteria.

Table 5.1 shows the statistics of the errors encountered using simple linear regression on first and second order terms of the reduced variable set. The average error is probably acceptable, but there are instances of large errors that would result in misclassification of the security. Fig. 5.2 plots the absolute and percentage errors for this linear estimator. The possibility of large errors for small margins can be seen. The designed ANN has a single hidden layer with 10 hidden nodes. There are 131 test cases of which 20% are used for testing. The overall performance is shown in Table 5.2. The results indicate very low percentage errors.

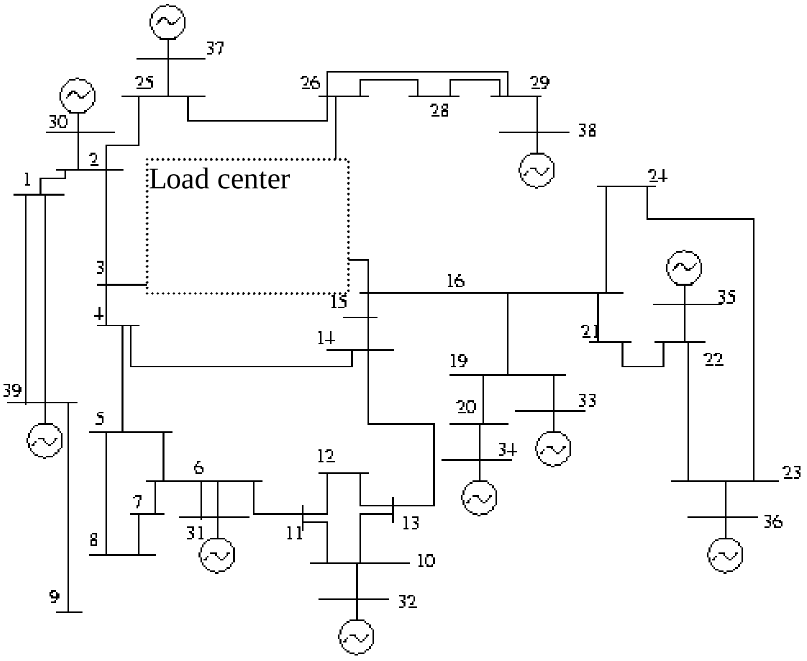


Fig. 5.1 New England 39 bus system

The second analysis is on estimation of the loading margin relative to transient frequency criteria (59.6 Hz – 6 cycles). The active and reactive power flows of all lines are used as the features to describe a system state. The ANN is trained using the data from the off-line operational studies. Initially, there are 96 total features (i.e., the active and reactive power flow of all the lines). These reduce to 31 features using principal components analysis. Statistical correlation coefficients were used to further reduce the dimension of the pattern vector to 11 elements. An ANN with 21 neurons in the single hidden layer was implemented using the Levenberg-Marquardt algorithm, and an ANN with 7 neurons of the single hidden layer was found to be adequate for Bayesian Regularization backpropagation. Since this is a rather small system, satisfactory performance is obtained using a simplified estimator of only one ANN.

The results, shown in Tables 5.2 and 5.3, indicate that more than sufficient accuracy is obtained using very small networks. The performance of the ANN using Bayesian Regularization algorithm is more accurate than the Levenberg-Marquardt algorithm. Further, since the Bayesian algorithm has fewer hidden neurons, training using this algorithm is faster in computation time.

Table 5.1 Errors from linear regression of voltage security limits for 39 bus system

Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/%)	Standard Deviation (MW)	MSE (MW^2)
52.04/52.04	0.02 / 0.002	10.92/2.37	13.61	185.16

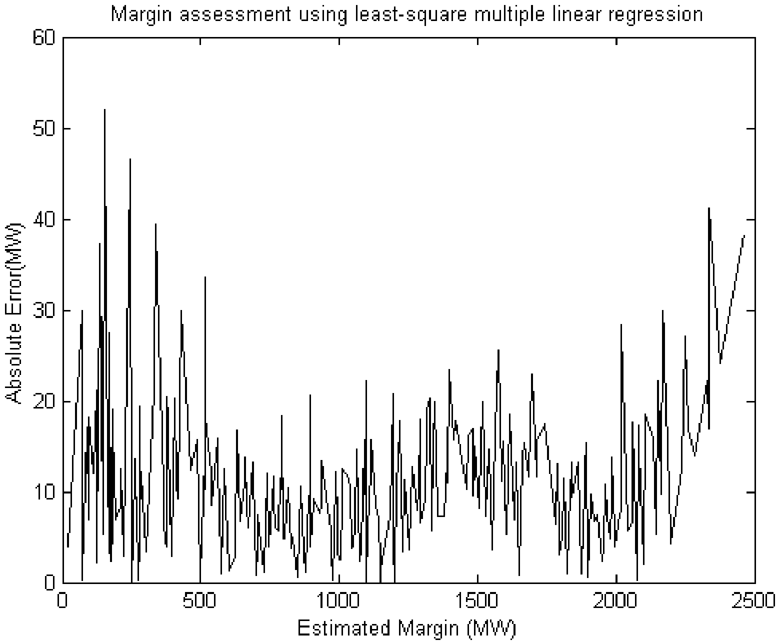
Table 5.2 Errors from ANN estimate of voltage security limits for 39 bus system

Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/%)	Standard Deviation (MW)	MSE (MW^2)
Levenberg-Marquardt				
2.95/2.50	0.0036/0.0005	0.63/0.15	0.73	0.72
Bayesian Regularization				
1.84/2.76	0.0011/0.0002	0.31/0.097	0.43	0.20

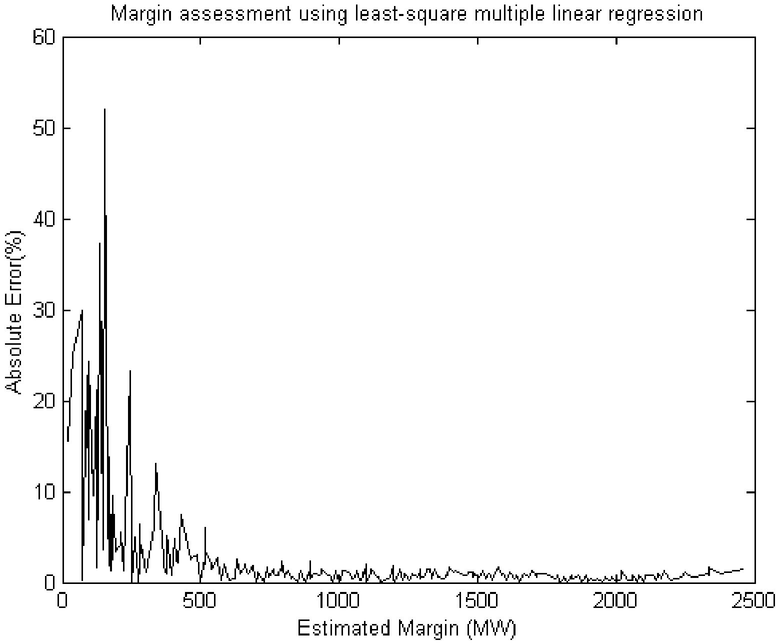
Table 5.3 Comparison of training routines on dynamic security estimator for 39 bus system

Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/ %)	Standard Deviation (MW)	MSE (MW^2)	Hidden neurons
Levenberg-Marquardt					
8.19/3.88	0.0024/0.0005%	0.49/0.15%	0.80	0.64	21
Bayesian Regularization					
1.07/1.90%	0.0014/0.0002%	0.15/0.11%	0.20	0.04	7

Fig. 5.3 and 5.4 show the plot the errors versus the magnitude of the voltage security margin. The errors are generally low where the margin tends to be large so there are no misclassifications of security. Fig. 5.5 and 5.6 show similar results for the dynamic security criteria. For the dynamic security, there is greater error near the lower margins, which could lead to misclassifications of security. However, the accuracy of the estimates for the voltage and dynamic security cases is more than adequate.

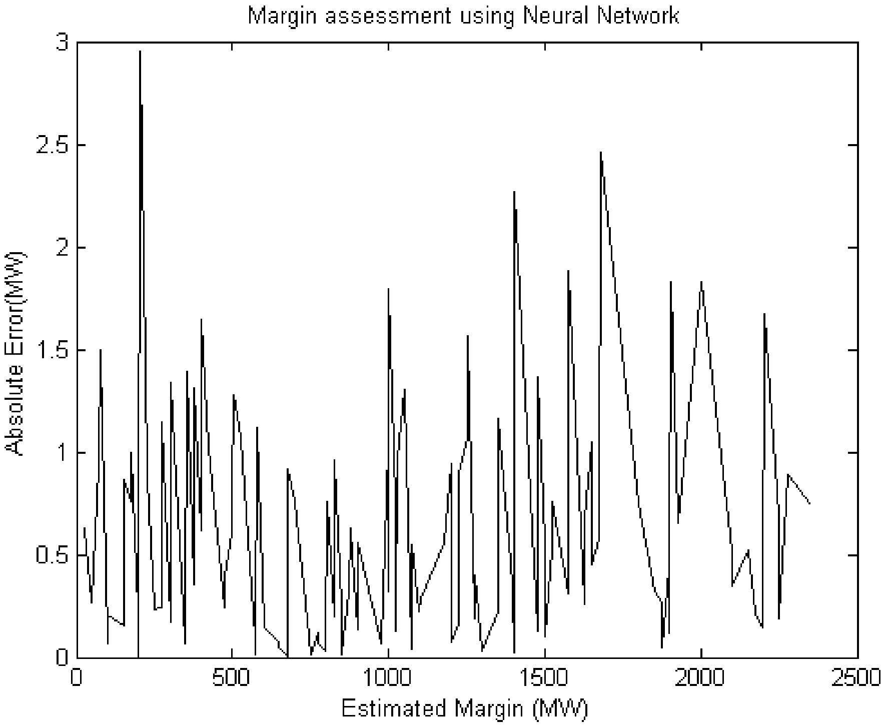


(a) MW error

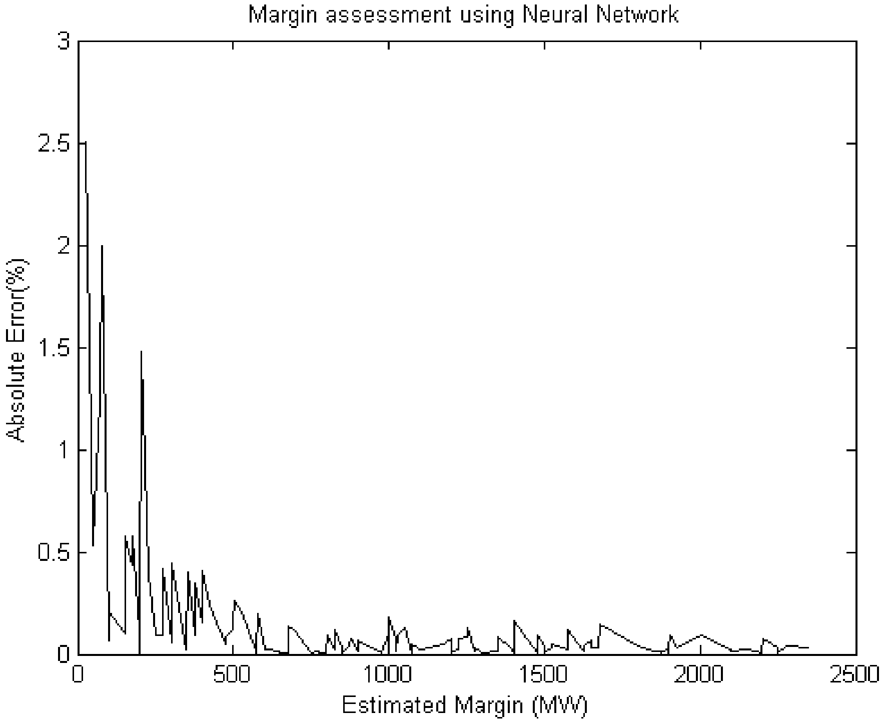


(b) % error

Fig 5.2 Voltage security margin estimates using linear regression for 39 bus system

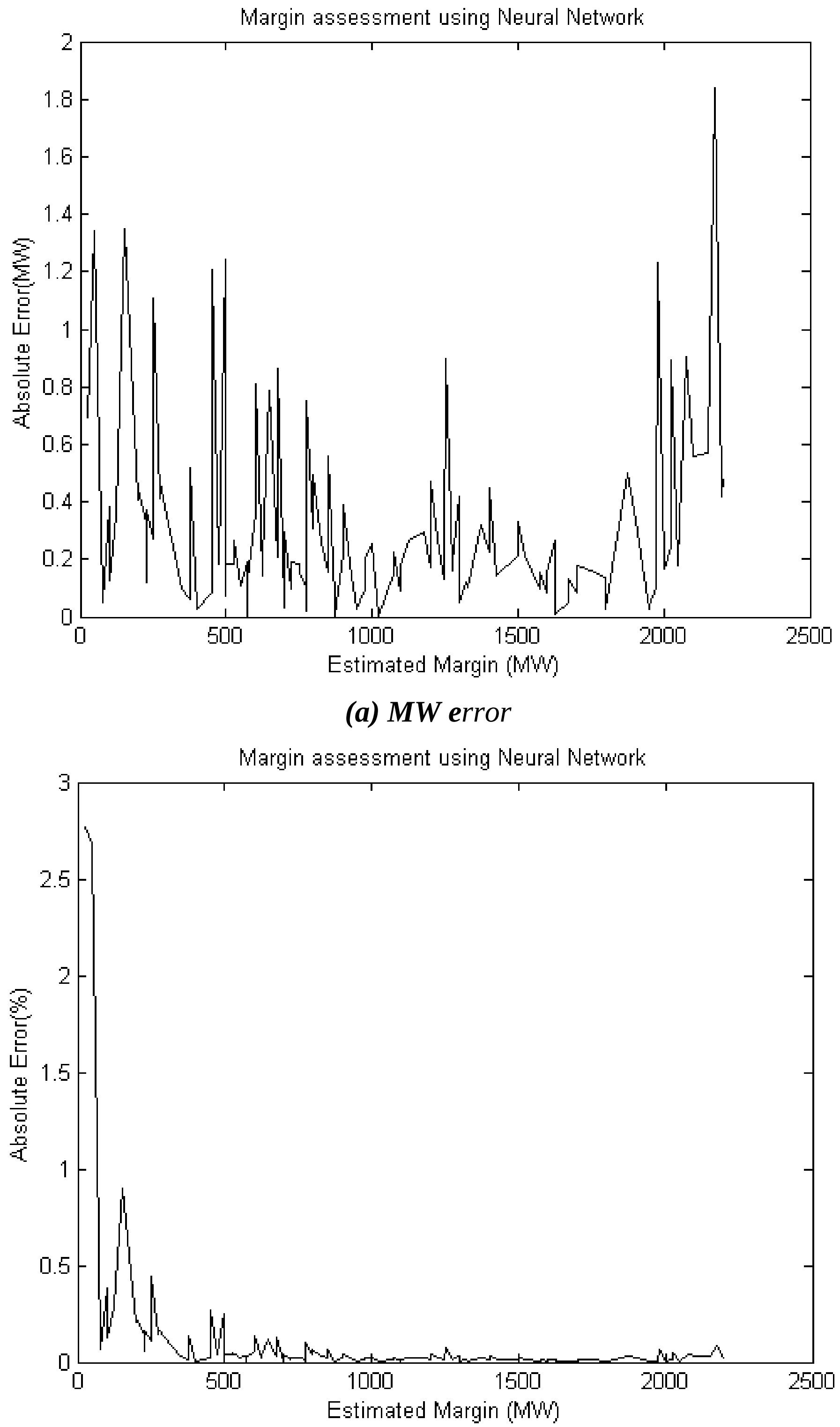


(a) MW error



(b) % error

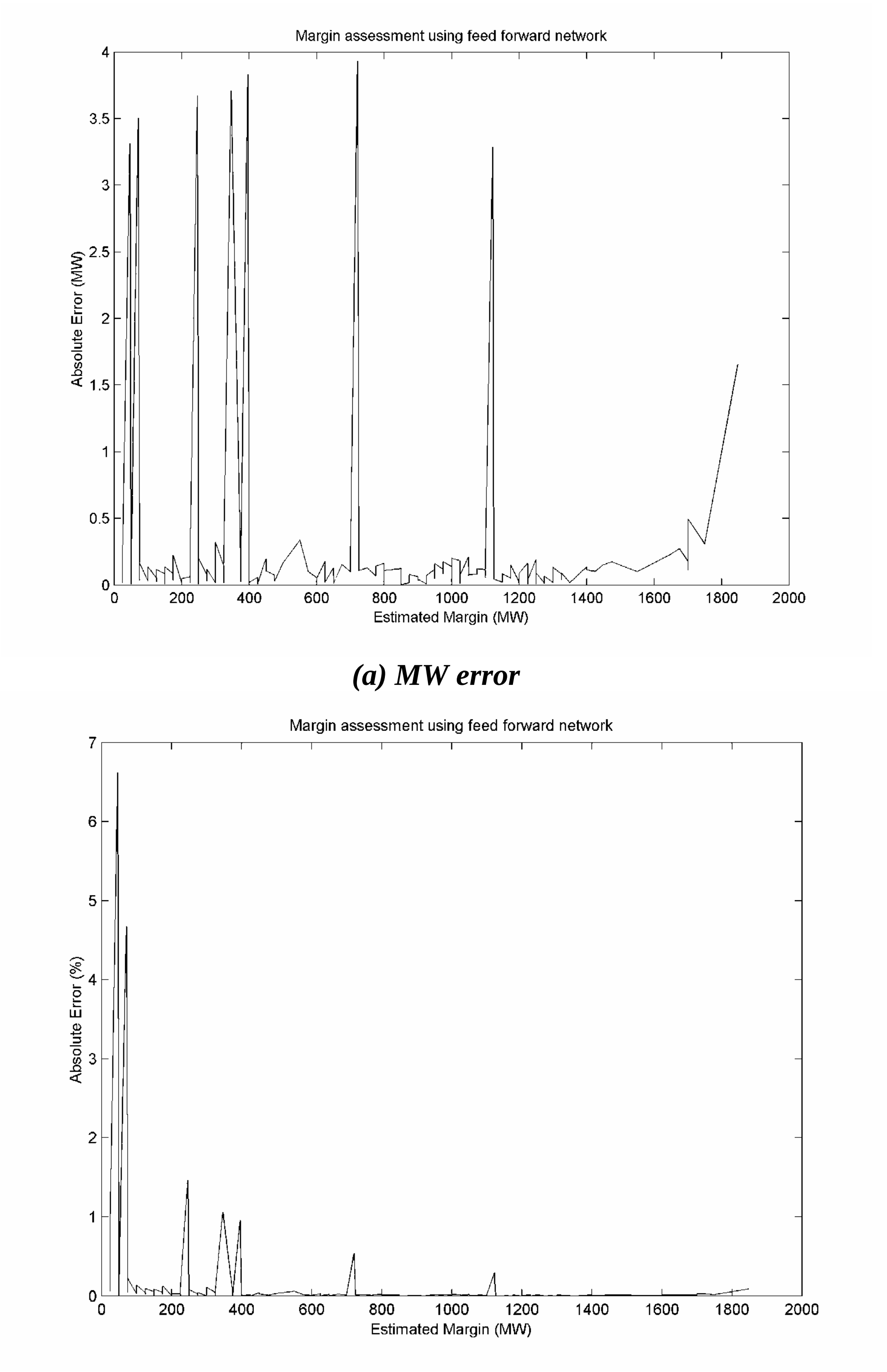
Fig. 5.3 Voltage security margin estimates using ANN with Levenberg-Marquardt training for 39 bus system



(a) MW e*rror*

(b) % error

Fig. 5.4 Voltage security margin estimates using ANN with Bayesian Regularization training for 39 bus system

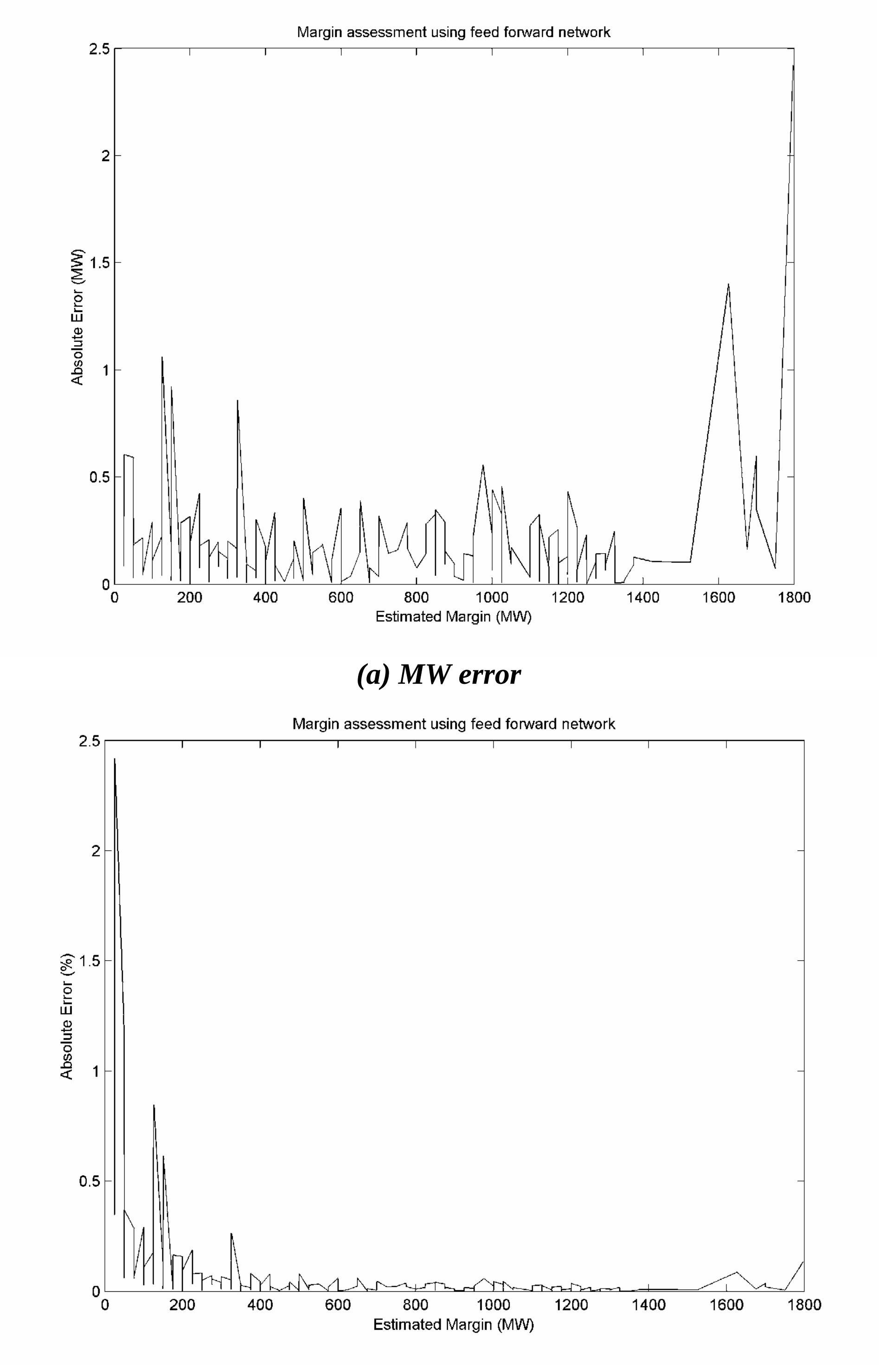


(a) MW error

(b) % error

Fig. 5.5 Dynamic security margin estimates using ANN with Levenberg-Marquardt for 39 bus system

The combination of PCA and correlation greatly reduced the number of needed features. This



(a) MW error

(b) % error

Fig. 5.6 Dynamic security margin estimates using ANN with Bayesian Regularization training for 39 bus system

implicitly assumes that the training truly captures salient characteristics of these features. Furthermore, data or training sets must be representative of the different states of the power system since ANNs are designed for interpolation not extrapolation.

5.2 Studies on WECC System Model

The proposed methodology was successfully applied to estimate the transfer limits on the WECC system using a static method, P-V curves, to determine voltage security limits [6]. In this section, application of the full performance level A criteria is examined.

5.2.1 System and Case Study Description

The Western Interconnection encompasses a vast area of nearly 1.8 million square miles. The Western Interconnection is defined as the Western Electric Coordinating Council (WECC) region, which is the largest and most diverse of the ten regional reliability councils of the North American Electric Reliability Council (NERC). It encompasses all or part of fourteen western states, two Canadian provinces, and portions of northern Mexico. It has characteristics that are distinct from the other three North American Interconnections. The WECC divides into four geographic subregions: California, Northwest, Arizona/New Mexico/Southern Nevada, and Rocky Mountain. About sixty percent of the WECC load is located in the coastal regions. A significant portion of the generation that serves these load centers is located inland, so transmission over long distances is needed. As a result, significant portions of the WECC network are stability limited. Fig. 5.7 shows the major transmission paths of the WECC system. The primary interface of interest in this study is the California-Oregon Intertie (COI). The COI consists of the two Malin-Round Mt. 500kV transmission lines (referred to as the Pacific AC Intertie) and the Captain Jack-Olinda 500kV line (referred to as the COTP).

To find the COI margin, generation in the Northwest area is scaled up while increasing loads in the California region. The minimum step size is 25 MW. For static voltage stability, VSTAB is employed. To find the margin for dynamic voltage stability and DSA, ETMSP version 5.0 is used. Software has been written to automate the process of evaluating the output of these simulation runs.

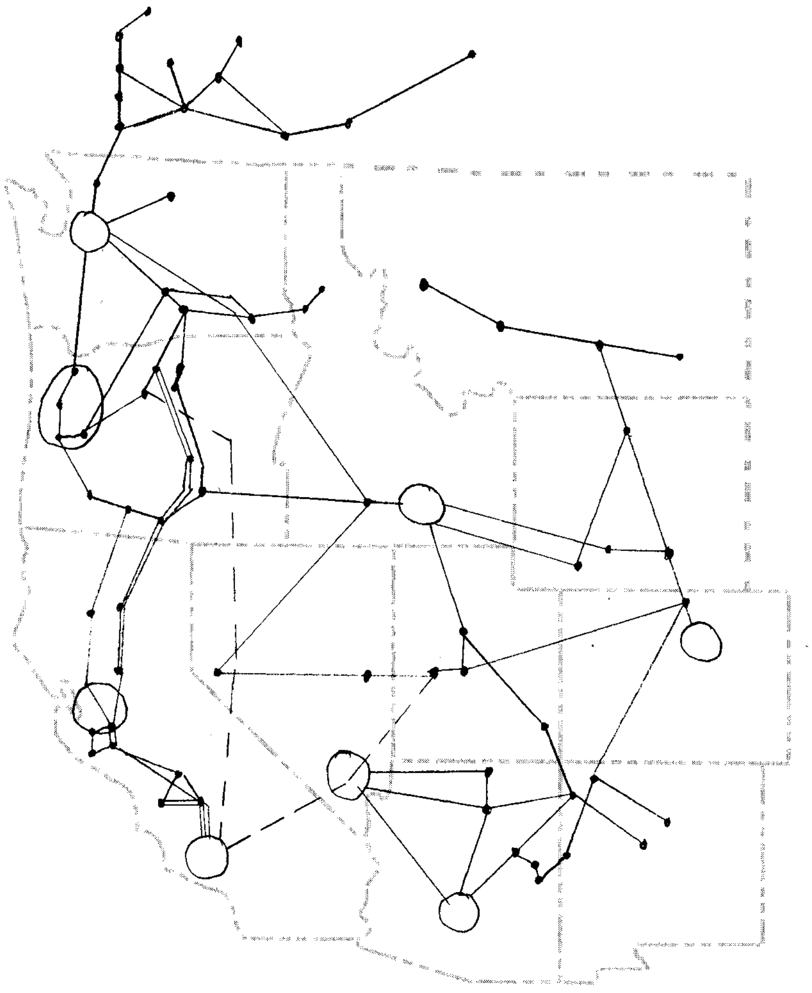


Fig. 5.7 Existing WECC major transmission lines and load centers

For the static margin, every 500kV line outage is studied. While for the dynamic margin, a three-phase fault on each 500kV line is studied. The fault duration is 0.15 second (9 cycles), which is longer than the normal clearing time. However, this duration facilitates our analysis. The system is simulated for 50 seconds following the fault. After the fault is cleared, the dynamic voltage reliability criteria for the 500kV buses are checked for any violation. If there is a violation, the system is considered dynamic unstable. The base case COI flow is 3400MW. A three-phase fault on each 500 KV line is considered. Eighty-four contingencies were selected for the studies. The 168 total features (i.e., the active and reactive power flow of all the lines) were reduced to 55 features using principal components analysis. Then, statistical correlation coefficients were used to reduce the dimension of the pattern vector to 17 elements.

Due to inconsistencies in the available data, different system models were used to evaluate static and dynamic security. The specific base case and study system used were as follows:

Dynamics: 1998 Spring 6000 bus system

Basecase COI flow: Actual 4600MW (COI flow is reduced to 3700MW in the voltage simulation studies and 3400 MW in transient stability studies for convenience of study and comparison)

Static voltage stability margin: 1995 Spring 4000 bus system
Basecase COI flow: 3700MW

5.2.2 Analysis

We begin by considering the voltage criteria. Table 5.4 shows the statistics of the errors encountered using simple linear regression on first and second order terms of the reduced variable set. In this case, both the average error and the maximum error are not acceptable, with a large number of instances that would result in misclassification. Fig. 5.8 plots the absolute and percentage error for this estimator and shows how several large errors occur for the low margin cases. The overall performance of the ANN approach for the voltage criteria is shown in Table 5.5, again using two training methods; however, a voting scheme for three networks of different dimensions is used to improve accuracy. These results are plotted in Figs. 5.9 and 5.10. The errors in the estimates are extremely low and would not lead to any misclassifications of security. Either of the two training approaches would be adequate, but Bayesian Regularization gives slightly superior results. This clearly establishes the effectiveness of this type of estimation.

Summary statistics are shown in Table 5.6. Figs. 5.11 and 5.12 show the relationship between margin and estimate error. The ANNs using Bayesian Regularization and Levenberg-Marquardt algorithm have similar performance with the Bayesian approach again showing slightly better performance. While most of the estimates are accurate, the low margin cases have larger errors. This is particularly troublesome because those are the cases where higher accuracy is most needed. There are a number of issues arising from these results.

1) Data generation: In this experiment, there is a problem with generating a sufficiently large population of dynamically insecure states for the WECC system. The fault-on period has been extended to find such cases. Still, only 84 insecure cases were found and these were poorly distributed. In the pattern matching approaches used in this project, data quality is the most important factor affecting performance.
2) ANN design: Another important issue is the choice of parameters as the input to the ANN. Our approach is to employ a voting scheme of networks with different network parameters. At this point, the limited data prevents this from providing significant improvement in performance.

Our on-going studies are focused on improving the routines for generation of the training set. The first step will be to consider heuristics and generic search algorithms to help find interesting cases. The current approach is essentially a random generation of a large numbers of studies that does not provide a systematic approach to finding insecure operating points. This approach may include biasing techniques to emphasize unusual cases that provide more information on system limits. Pattern matching approach works well in interpolation but cannot extrapolate to the find limits. It is important to guide the data generation to capture the breadth of the operating range.

Table 5.4 Errors from linear regression of voltage security limits for WECC bus system

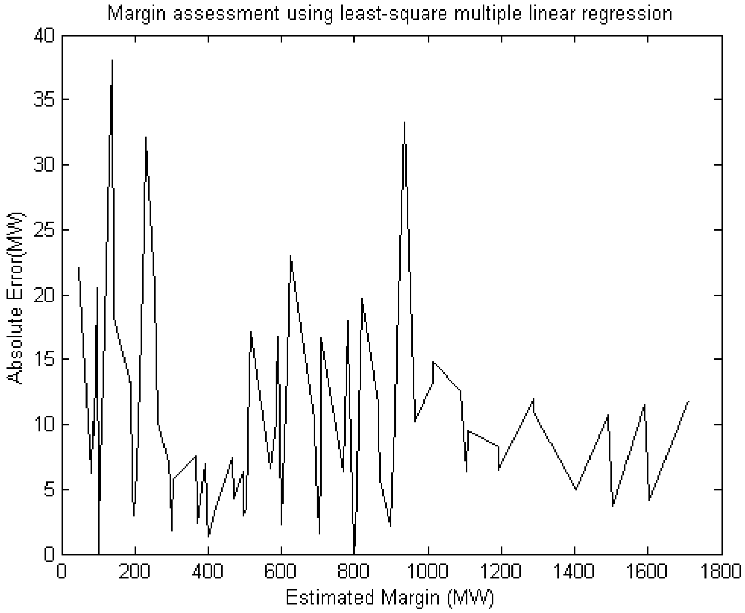
Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/%)	Standard Deviation (MW)	MSE (MW^2)
38.1/88.4%	0.11/0.027%	9.60/3.33%	11.60	138.70

Table 5.5 Errors from ANN estimate of voltage security limits for WECC bus system

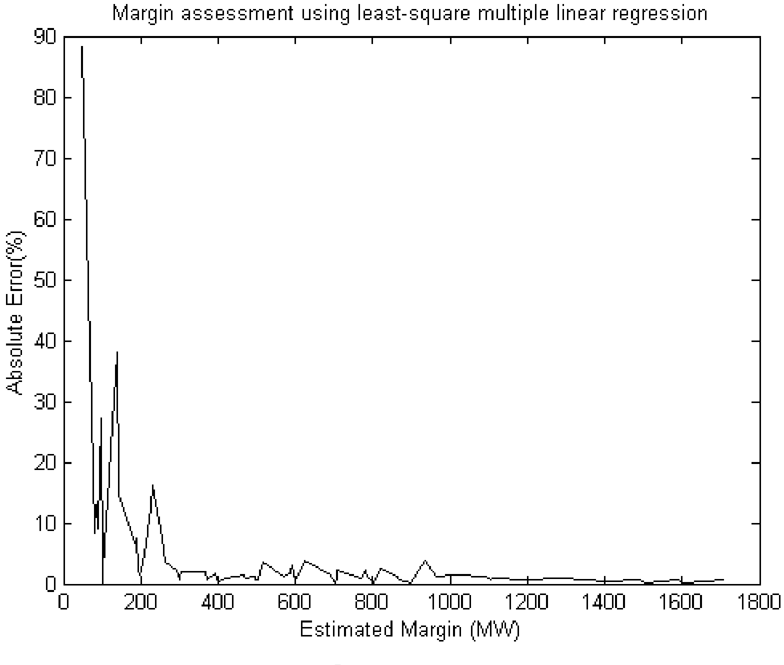
Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/%)	Standard Deviation (MW)	MSE (MW^2)
Levenberg-Marquardt				
31.72/6.86	0.046/0.0046	4.58/0.92	7.94	64.14
Bayesian Regularization				
12.64/3.48	0.024/0.0027	1.84/0.39	3.30	10.80

Table 5.6 Comparison of training routines on dynamic security estimator for WECC bus system

Max Error (MW/%)	Min Error (MW/%)	Mean Error (MW/ %)	Standard Deviation (MW)	MSE (MW^2)	Hidden neurons
Levenberg-Marquardt					
73.61/53.34	0.014/0.0029	11.28/4.07%	16.68	278.76	30
Bayesian Regularization					
95.77/85.50	0.005/0.0006	8.78/4.34	18.30	333.45	24

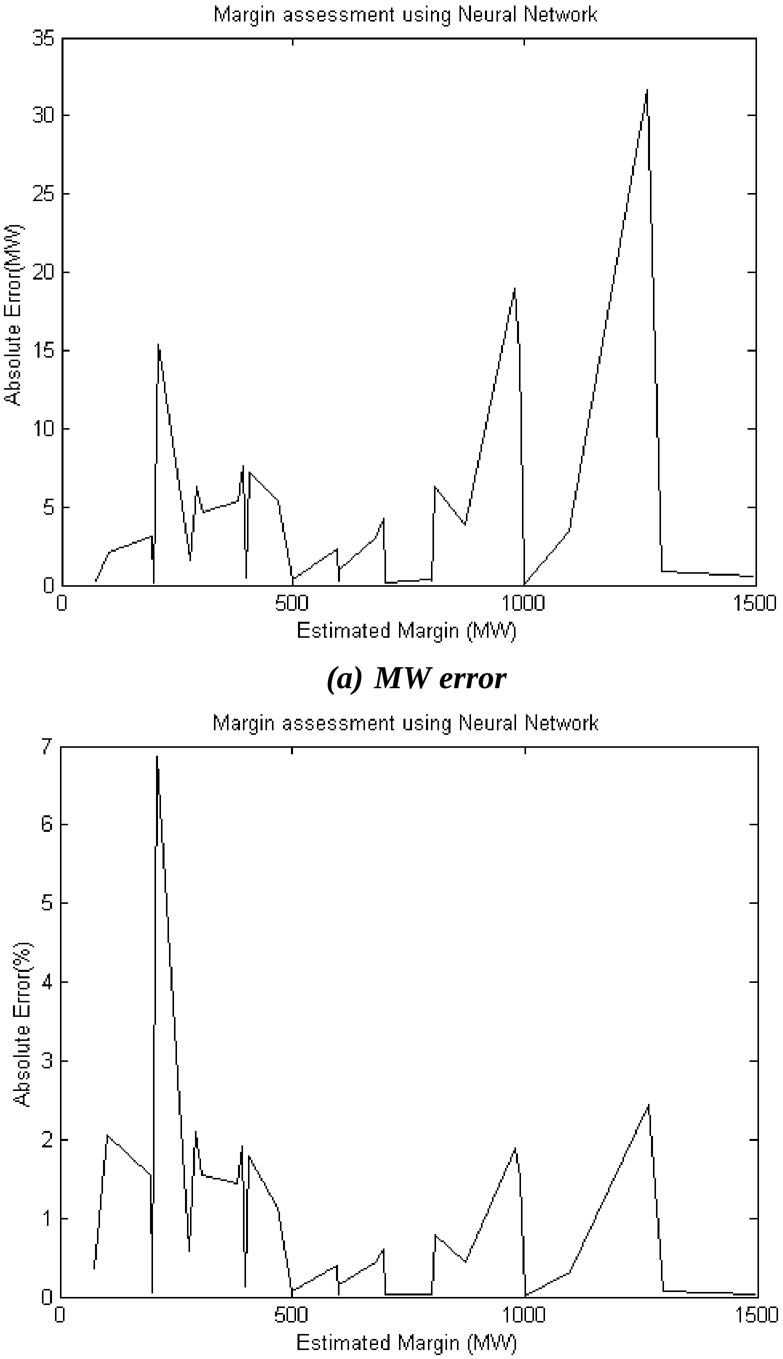


(a) MW error



(b) % error

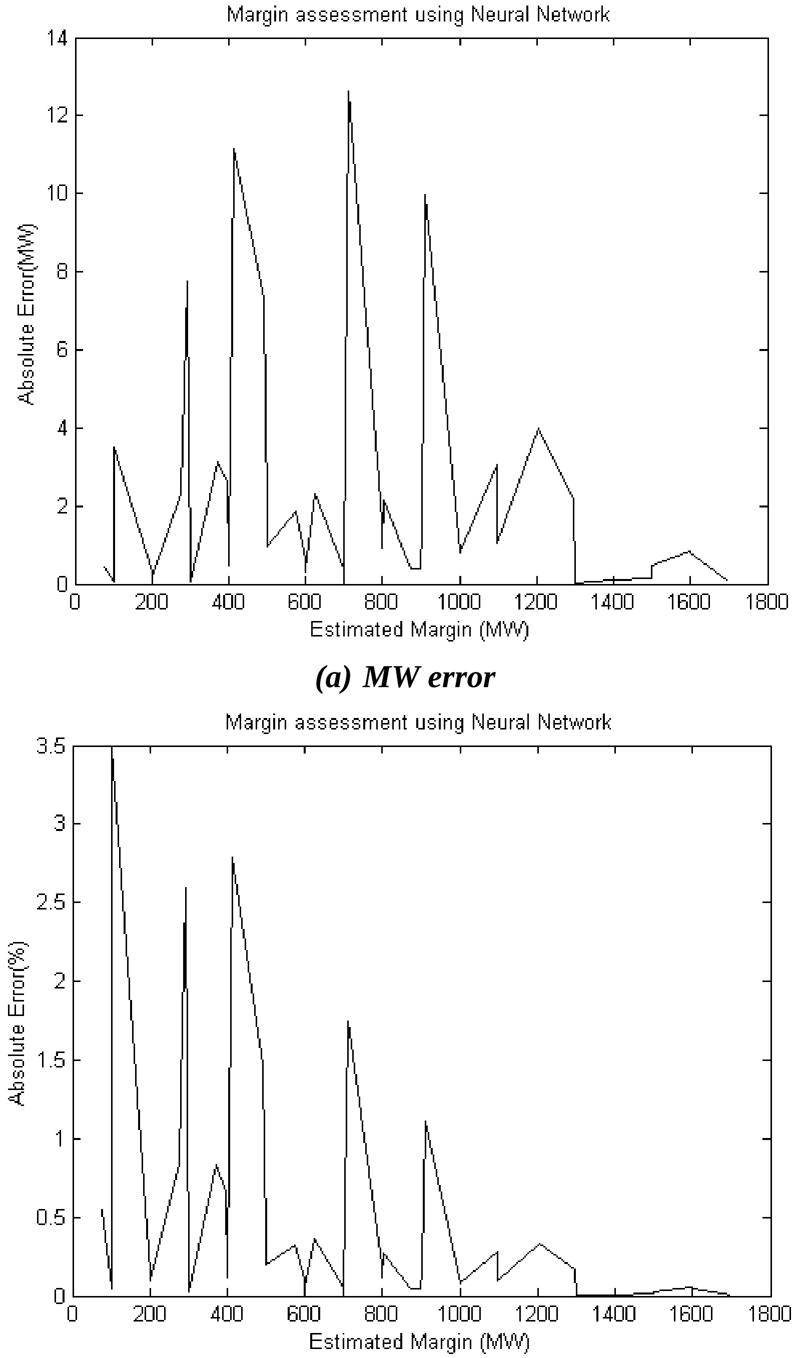
Fig. 5.8 Voltage security margin estimates using linear regression for WECC system



(a) MW error

(b) % error

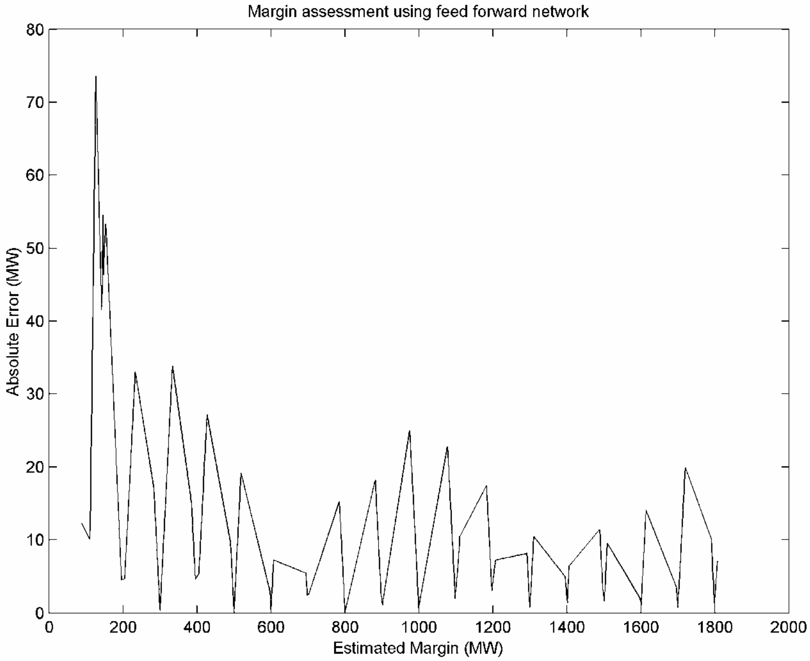
Fig. 5.9 Voltage security margin estimates using ANN with Levenberg-Marquardt training for WECC system



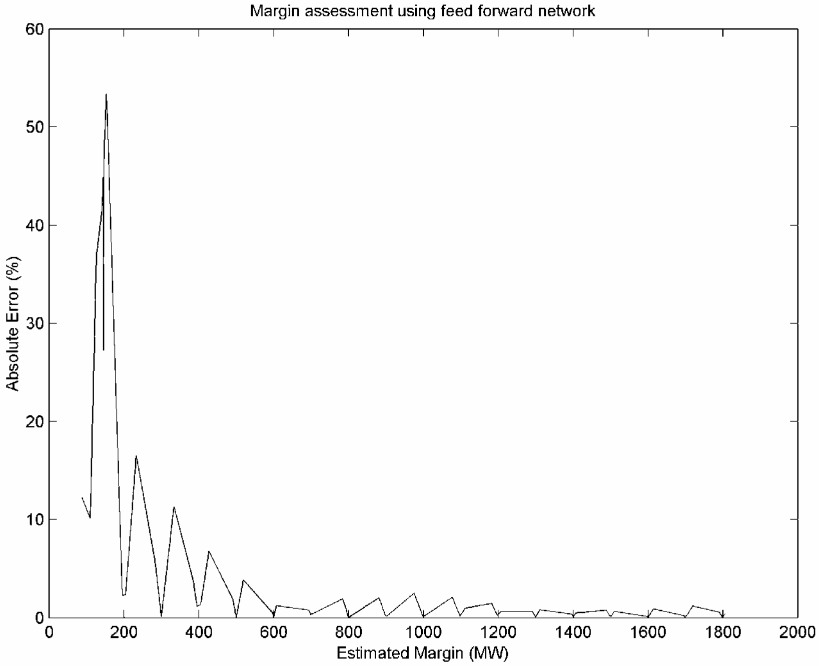
(a) MW error

(b) % error

Fig. 5.10 Voltage security margin estimates using ANN with Bayesisan Regularization training for WECC system

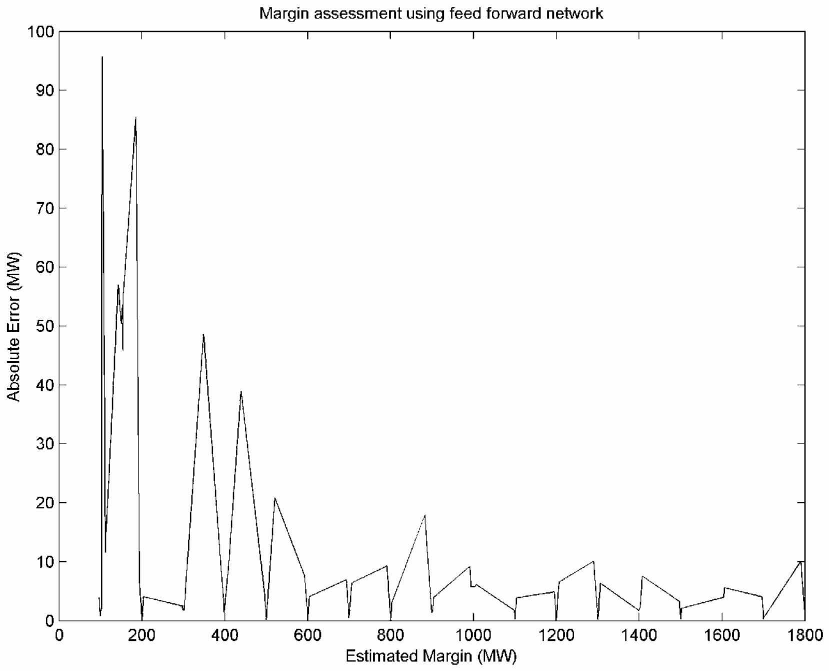


(a) MW error

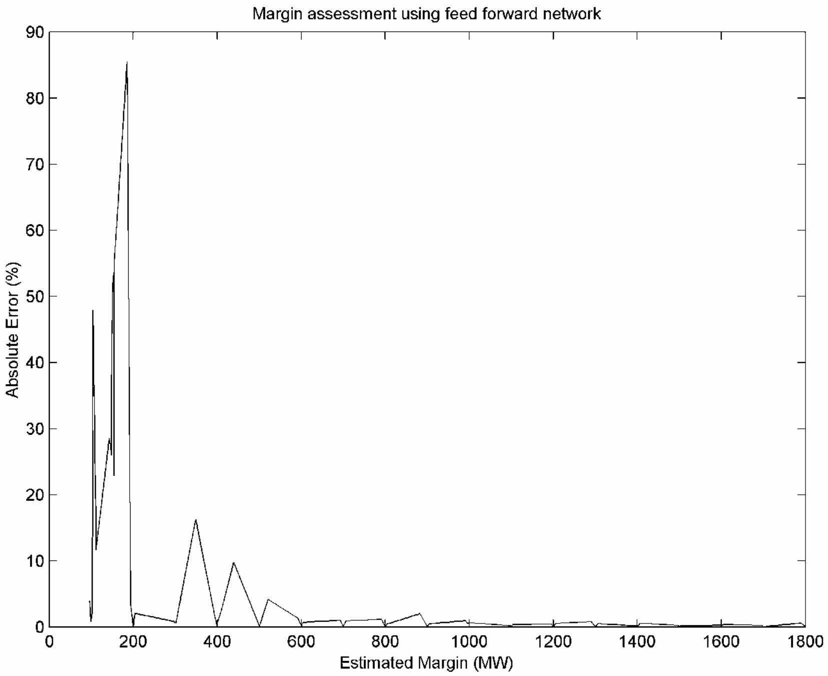


(b) % error

Fig. 5.11 Dynamic security margin estimates using ANN with Levenberg-Marquardt training for WECC system



(a) MW error



(b) % error

Fig. 5.12 Dynamic security margin estimates using Bayesian Regularization training for WECC system

6. Conclusions and Future Studies

This study developed and analyzed an integrated framework employing ANNs to estimate on-line security. The primary advantage of the approach is in:

- making full use of the numerous detailed off-line studies performed during operations planning,
- providing a simple intuitive assessment of security for operators, and
- allowing for any security index that may be of use for a particular system, including system specific indices.

Prediction and generalization capabilities of these ANNs provide a flexible mapping of input attributes to the single-valued space of the security margin. Because ANNs have high computation rates, they are an excellent tool for on-line application. This conclusion holds particularly when either data requirements and/or the computational burden have rendered other approaches impractical for implementation.

The results obtained from the 39 bus system showed that our integrated approach was able to predict the security margin with a high degree of accuracy for the complete security assessment problem. In our previous work, we showed that this methodology works for the static security assessment of large practical systems. This project subsequently demonstrates the feasibility of obtaining similar estimates for dynamic security assessment. While the 39 bus results appeared promising, the difficulty in implementing these approaches is in large system applications. While some additional analysis is needed, the full complex models used for the WECC system establish that the approach is practical.

Perhaps the main concern with our approach is the added burden it places on operational planning. These off-line simulation studies are extremely time-consuming. This has been addressed somewhat in our approach by automating the process of applying reliability criteria to the simulation results. Yet, experienced operational planners are far more efficient in their use of simulation tools because of their choice of studies; however, that approach can mislead operators dealing with unusual loading conditions. Finally, the method we propose can only be as good or complete as the off-line analyses. If models are incorrect, or if highly unusual load patterns arise, the estimates will be suspect. Finally, as was seen for transient stability of the WECC, if the number of informative cases (i.e., unstable cases) are small and poorly distributed, then poor estimates will occur.

6.1 Significant Contributions

This project produced a number of contributions to the development dynamic security analysis techniques.

- A comprehensive framework was developed for on-line estimation of security margins, calculated based on current operating practices.
- The framework proposed families of estimators, each specialized for specific system limits and the appropriate security criteria (i.e., static, dynamic or voltage). The

estimators can be combined to provide an overall assessment of system operating conditions.

- A system of estimators was implemented and tested on a modified New England 39 bus system.
- Based on the insights from the New England system, a more sophisticated set of estimators was implemented and tested on a 6000 bus model of the Western Area system. The focus of this study was the California-Oregon Intertie transfer limits.
- A number of software tools were developed to help automate the process of evaluating security margins in off-line studies.
- The results show that it is possible to very accurately estimate security margins for large systems on-line. The main limitation of the approach resides in the ability of time-consuming off-line studies to accurately model system dynamics.

6.2 Recommended Further Developments

A number of efforts are needed to develop this integrated security analysis approach into a workable and efficient dynamic security assessment tool for large systems.

1. Improved generation of study data: Currently, the studies are essentially exhaustive. While some planning and operator experience is implicitly included due to the chosen reliability criteria, greater inclusion of such experience could reduce the needed computation time. For example, many security problems only arise under specific operating conditions. Such insight could be used to reduce the number of study cases. The analysis of the system response has been automated to a certain extent, but there are peculiarities that require case-by-case analysis. These can be quite time-consuming to address individually.
2. Use of alternative indices: This study employed the most detailed models available and used time domain analysis. The motivation was to avoid controversy that may be associated with the value of approximating some less than precise index. There are certainly many useful techniques, most notably energy function methods and transient stability indices, that could be considered. The value of our proposed approach lies in improved computationally efficiency for on-line application.
3. Improved estimators: While the performance of the developed estimator appears more than adequate for most applications, a number of improvements could be made, including:
    a. Dynamically updating the estimators based on the current operating conditions or new studies
    b. Exploring select sets of features that work across different operating situations, thus simplifying estimator design
    c. Grouping of data to identify similar operating conditions to possibly reduce the number of required estimators.
4. Suggested corrective action: The estimators could be used to identify generation adjustments or other corrective actions to increase security margins. In fact, they could be easily employed to form a security constrained Optimal Power Flow.
5. Improved operator interface: This work did not investigate closely operator issues associated with the use of the selected estimators. For example, because the estimates are computed essentially instantaneously, an operator could easily use the estimators to quickly verify that a remedial action does not lead to other security violations.

7. Description of Study Data and Developed Software

This section summarizes the software developed and example data generated for this study.

System study data:

Modeling: ETMSP dynamic models data, disturbance descriptions, output descriptions (for modified 39 bus and WECC 4000 and 6000 bus models).

Results: Power flow solutions for all study cases, calculated security margins for all indices and study cases (for modified 39 bus and WECC 4000 and 6000 bus models). These results are stored in Matlab data files.

Margin calculation:

Contingency List: Several files and routines are needed for generating the complete list of contingencies for the system under study and varying the system load and generation pattern.

Output analysis: The ETMSP output is read into Matlab where it is analyzed for conformance with WECC criteria. Each case is represented by a set of representative features, including real and reactive power flows on all major transmission lines. These results are stored in a database.

Estimator design:

Data analysis: Routines for computation of correlation coefficients and principal component analysis.

Estimator: Routines for training a neural net using Levenberg-Marquardt and Bayesian Regularization backpropagation and the resulting estimators for the system studies.

8. References

[1] G. W. Stagg and A. H. El-Abiad, “Computer Methods in Power Systems Analysis,” McGraw Hill, New York, NY, 1968.

[2] T. E. DyLiacco, “The Adaptive Reliability Control System,” IEEE Transactions on Power Apparatus and Systems, Vol. PAS-86m No. 5, 1967, pp. 517-531.

[3] *Automated Operating Procedures for Transfer Limits*, Final Report, PSerc Publication 01-05, May 2001.

[4] A.A. EI-Keib and X. Ma, “Application of Artificial Neural Networks in Voltage Stability Assessment,” *IEEE Transactions on Power System*, Vol. 10, No.4, Nov. 1995, pp. 1890-1896.

[5] S. Chauhan and M.P. Dava, “Kohonen Neural Network Classifier for Voltage Collapse Margin Estimation,” *Electric Machines and Power Systems*, Vol. 25, No. 6, July 1997, pp. 607-619.

[6] L. Chen, K. Tomsovic, A. Bose and R. Stuart, “Estimating Reactive Margin for Determining Transfer Limits,” accepted for *IEEE Transactions on Power Systems*.

[7] S. Haykin, *Neural Networks, a Comprehensive Foundation*, 2nd Edition, Prentice Hall, 1999, New Jersey.

[8] C. W. Taylor, *Power System Voltage Stability*, McGraw-Hill, 1994, New York.

[9] Western Systems Coordinating Council, *Reliability Criteria*, Aug. 2000.

[10] IEEE Committee Report, “Dynamic Security Assessment Practices in North America,” *IEEE Transactions on Power Systems*, Vol. 3, No. 3, August 1988, pp. 1310-1321.

[11] H. W. Dommel and N. Sato, “Fast Transient Stability Solutions,” IEEE Transactions on Power Apparatus and Systems, Vol. 91, July/August 1972, pp. 1643-1650.

[12] M. Ribbens-Pavella and F. J. Evans, “Direct Methods for Studying Dynamics of Large-Scale Electric Power Systems – A survey,” *Automatica*, Vol. 21, No. 1, 1985, pp. 1-21.

[13] A. D. Patton, “Assessment of the Security of Operating Electric Power System using Probability Methods,” Proceedings of IEEE, Vol. 62, No. 7, July 1974.

[14] H. Hakim, “Application of Pattern Recognition in Transient Security Assessment,” Journals of Electrical Machines and Power Systems, Vol. 20, 1992, pp. 1-15.

[15] L. Wehenkel, *Automatic Learning Techniques in Power Systems*, Kluwer Academic Publishers, MA, 1998.

[16] A. Tiranuchit and R. J. Thomas, "A Posturing Strategy Against Voltage Instabilities in Electric Power Systems", *IEEE Transactions on Power Systems*, Vol. 3, No. 1, Feburary 1998, pp.87-93.

[17] C. A. Canizares, F. L. Alvarado, C. L. DeMarco, I. Dobson and W. F. Long, "Point of Collapse Method Applied to AC/DC Power Systems", *IEEE Transactions on Power Systems*, Vol. 7, No. 2, May 1992, pp. 673-683.

[18] T. Van Cutsem and C. Vournas, *Voltage Stability of Electric Power Systems*, Kluwer Academic Publishes, Boston, 1998.

[19] W. Rosehart, C. Canizares and V. Quintana, "Optimal power flow incorporating voltage collapse constraints," *Proceedings of the 1999 IEEE PES Summer Meeting*, July 1999, Vol. 2, pp. 820-825**.**

[20] Western Systems Coordinating Council, *Voltage Stability Criteria, Undervoltage Load Shedding Strategy, and Reactive Power Reserve Monitoring Methodology*, May 1998.

[21] M. Moechtar, T. C. Cheng, and L. Hu, "Transient Stability of Power System – A Survey," *WESCON Conference Record Proceedings of 1995*, San Francisco, California, Nov. 7-9, 1995, pp. 166-171.

[22] D. Sobajic, and Y. Pao, "Artificial Neural Net Based Dynamic Security Assessment for Electric Power Systems," *IEEE Transactions on Power Systems*, Vol. 4, No. 1, February 1989, pp. 220-228.

[23] Y. Pao, and D. J. Sobajic, "Combined Use of Unsupervised and Supervised Learning for Dynamic Security Assessment," *IEEE Transactions on Power Systems*, Vol. 7, No. 2, February 1989, pp. 878-884.

[24] M. A. El-Sharkawi, R. J. II Marks, M. E. Aggoune, D. C. Park, M. J. Damborg, and L. E. Atlas, "Dynamic Security Assessment of Power Systems Using Back Error Propagation Artificial Neuron Networks," *Proceedings of the 2nd Symposium on Expert System Applications to Power Systems*, Seattle, WA, July 1989.

[25] R. Kumar, A. Ipahchi, V. Brandwajan, M. A. El-Sharkawi, and G. Cauley, "Neuron Networks for Dynamic Security Assessment of Large Scale Power Systems: Requirements Overview," *Proceedings of 1st International Forum on Applications of Neuron Networks to Power Systems*, Seattle, WA, July 1991, pp. 65-71.

[26] Y. Mansour, A. Y. Chang, J. Tamby, E. Vaahedi, B. R. Corns, and M. A. El-Sharkawi, "Large Scale Dynamic Security Screening and Ranking Using Neuron Networks," *IEEE Transactions on Power Systems*, Vol. 12, No. 2, May 1997, pp. 954-960.

[27] H. P. St. Clair, "Practical Concepts in Capability and Performance of Transmission Lines", *AIEE Transactions*, Vol. 72, 1953, pp. 1152-1157.

[28] R. D. Dunlop, R. Gutman, and P. P. Marachenko, "Analytical Development of Loadability Characteristics for EHV and UHV Transmission Lines", *IEEE Transactions on Power Apparatus and Systems*, Vol, PAS-98, No. 2, March/April 1979, pp. 606-617.

[29] T. W. Kay, P. W. Sauer, R. D. Shultz, and R. A. Smith, "EHV and UHV Line Loadability Dependence on VAR Supply Capability", *IEEE Transactions on Power Apparatus and Systems*, Vol. PAS-101, No. 9, September, 1982, pp. 3568-3575.

[30] S. Grijalva and P. W. Sauer, "Reactive Power Considerations in Linear ATC Computation", *Decision Support Systems, The International Journal*, North-Holland, Elsevier, Vol. 30, 2001, pp. 327-340.

[31] *Interactive Power Flow User's Manual*, EPRI TR-103643-V2, prepared by Ontario Hydro, October 1994.

[32] *VSTAB Version 4.0 User's Manual*, prepared by Ontario Hydro.

[33] *ETMSP Version 5.0 User's Manual*, prepared by Ontario Hydro.

[34] D.J.C. MacKay, "Bayesian Interpolation," *Neural Computatio*n, Vol. 4, No. 3, 1992, pp. 415-447.

[35] S. Amari, N. Murata, K.-R. Muller, M. Finke, and H. Yang, "Statistical Theory of Overtraining - Is Cross-validation Asymptotically Effective*?" Advances in Neural Information Processing Systems*, Vol. 8, Cambridge, MA: MIT Press, 1996, pp. 176-182.

Appendix A Integrated Security Analysis (ISA) Tools Survey

A.1 Survey form

CERTS
CONSORTIUM FOR ELECTRIC RELIABILITY TECHNOLOGY SOLUTIONS

Integrated Security Analysis Tools Survey Form

Evaluator: **Date:**

1 General Information

1.1 Contact

Organization:	Person:	Position:
Address:	Phone:	E-mail:

Is the organization (circle one): investor owned, public, RTO/ISO, security coordinator?
Can we sight you and your organization in the survey report?

1.2 Analysis Tools Information

Primary Vendor:	Installation Date:	Version:	OS Platform:

2 Support Functions

2.1 Power System Model

No. Substations:	No. Busbars:	No. Generators:
No. Lines:	UpdateFrequency (days):	Neighbor Model Exchange (Y/N):
Format (PSSE, PSLF…):	Vendor Name or Custom:	Effectiveness/Robustness (1-10):

Issues/Plans:

2.2 Network Reduction

No. Buses:	No. Lines:	Online/Offline:	Update Frequency (days):
Neighbor Equivalence Exchange (Y/N):	Format (PSSE, PSLF…):	Frequency of Exchange (days):	Vendor Name or Custom:

Effectiveness/Robustness (1-10):

Issues/Plans:

2.3 SCADA

No. Status Pts & Scan Rate:	No. Analogs & Scan Rate:	No. ICCP Pts & Scan Rate:	Vendor Name or Custom:

Effectiveness/Robustness (1-10):

Issues/Plans:

2.4 Power Flow

Operational, Not Used, or Unavailable:	On-line or Offline:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
Issues/Plans:			

2.5 State Estimation

Operational, Not Used, or Unavailable:	On-line or Offline:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
Update Frequency (min):			
Issues/Plans:			

3 Security Analysis Functions

3.1 Contingency Analysis

Operational, Not Used, or Unavailable:	On-line or Offline:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
No. Contingencies Screened:	No. Contingencies Full Power Flow:	Update Frequency (min):	Typical Exec. Time (sec):
Primary Purpose or Need/Issues/Plans:			

3.2 Security Constrained Dispatch

Operational, Not Used, or Unavailable:	Manual Control or Automatic:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
Update Frequency (min):		Typical Exec. Time (sec)	
Primary Purpose or Need/Issues/Plans:			

3.3 Optimal Power Flow (OPF)

Operational, Not Used, or Unavailable:	On-line or Offline:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
Update Frequency (min):		Typical Exec. Time (sec):	
Primary Purpose or Need/Issues/Plans:			

3.4 Security Constrained OPF

Operational, Not Used, or Unavailable:	On-line or Offline:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
Update Frequency (min):		Typical Exec. Time (sec):	
Primary Purpose or Need/Issues/Plans:			

3.5 Voltage/VAR Dispatch

Operational, Not Used, or Unavailable:	Open or Closed Loop:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
Update Frequency (min):		Typical Exec. Time (sec):	
Primary Purpose or Need/Issues/Plans:			

3.6 Transient Stabilty Analysis

Operational, Not Used, or Unavailable:	On-line or Offline:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
No. Contingencies Screened:	No. Contingencies Full Analysis:	Update Frequencey (min):	Typical Exec. Time (sec):
Primary Purpose or Need/Issues/Plans:			

3.7 Mid-Term Stability Analysis

Operational, Not Used, or Unavailable:	On-line or Offline:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
No. Contingencies Screened:	No. Contingencies Full Analysis:	Update Frequencey (min):	Typical Exec. Time (sec):
Primary Purpose or Need/Issues/Plans:			

3.8 Long-Term Stability Analysis

Operational, Not Used, or Unavailable:	On-line or Offline:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
No. Contingencies Screened:	No. Contingencies Full Analysis:	Update Frequencey (min):	Typical Exec. Time (sec):
Primary Purpose or Need/Issues/Plans:			

3.9 Eigenvalue Analysis

Operational, Not Used, or Unavailable:	On-line or Offline:	Vendor Name or Custom:	Effectiveness/ Robustness (1-10):
No. Contingencies Screened:	No. Contingencies Full Analysis:	Update Frequencey (min):	Typical Exec. Time (sec):
Primary Purpose or Need/Issues/Plans:			

A.2 Survey Data Synthesis

Integrated Security Analysis (ISA) Tools Survey Data Synthesis

1. Description of the Integrated Security Analysis Tools

Acronym	Function	Description
Model	Power System Model	Off-line tool for creating and maintaining power system models. This includes importing and exporting using different data formats, data validation, and moving data into the operational system.
NR	Network Reduction	A tool to create a reduced model at the boundary of an area of interest with a behavior similar to a complete representation when studying changes in the area of interest. NR is used to obtain an equivalent of the external network belonging to neighboring organizations. The equivalent is used in the on-line system by network security analysis functions. NR is traditionally run off-line; however, real-time adjustments to equivalents are also possible.
SCADA	Supervisory Control and Data Acquisition	A subsystem used to acquire measurement information from the operational power system and process it for display it to the system operators. This includes data processing to convert and calculate new information, alarming of limit violations, and supervisory control of switches, taps, and generator set points.
PF	Power Flow	Study function for steady-state analysis of changes of state in power system equipment, including changes in generation, changes in load, and equipment outages. Also used to calculate network loss factors. The results of PF may be used as base case starting points for security analysis functions.
SE	State Estimation	An on-line determination of the operating state of the power system through statistical estimation methods by fitting a redundant set of real-time SCADA measurements with the power system model. This includes observability, state monitoring, anomaly detection, network parameter update, and busload flow forecast.
SCA	Static Contingency Analysis	A steady state determination of those changes (contingencies) to the system that result in equipment overload or abnormal voltage conditions in the network. Generally, SE provides the starting point (base case condition) for the analysis. This includes contingency screening (a fast, simplified selection process to determine potentially harmful contingencies), as well as a full, steady state analysis of contingent states.
SCD	Security Constrained	The optimal dispatch of generation and other controller moves whose objective is to prevent an overload condition

	Dispatch	upon the occurrence of a contingency. A form of OPF is used to calculate security constrained commands and selected contingencies
OPF	Optimal Power Flow	A general-purpose optimization tool to study a number of objective functions including power transfer capability, wheeling transfer evaluation, and power loss minimization. Depending upon the nature of the objective, linear or non-linear solution techniques are employed. The solution core of the OPF is often used for SCD, VVD, and SCOPF. The analysis presumes steady-state operation.
SCOPF	Security Constrained OPF	A form of OPF that recognizes contingency constraints in recommending controller moves. The tool is often used to recommend remedial (preventative) action prior to a contingency occurring.
VVD	Voltage VAR Dispatch	An optimal dispatch tool (with minimal control action) to meet network voltage profile requirements by recommending controls to reactive devices (generators, capacitors, reactors, transformer taps, etc.).
TSA	Transient Stability Analysis	TSA provides short-term transient reaction of the system to contingent conditions. In an operating environment, TSA explores many pre-specified contingencies. As with CA, contingencies are often screened with fast techniques. Potentially harmful contingencies are then examined with a more complete analysis.
MSA	Mid-term Stability Analysis	MSA provides mid-term dynamic reaction of the system to contingent conditions. In an operating environment, MSA explores many pre-specified contingencies. As with CA, contingencies are often screened with fast techniques. Potentially harmful contingencies are then examined with a more complete analysis.
LSA	Long-term Stability Analysis	LSA provides long-term dynamic reaction of the system to contingent conditions. In an operating environment, LSA explores many pre-specified contingencies. As with CA, contingencies are often screened with fast techniques. Potentially harmful contingencies are then examined with a more complete analysis.
EIG	Eigenvalue Analysis	Eigenvalue analysis looks at the harmonic interactions between modeled components of the power system (electrical and mechanical) to determine damped (stable) or un-damped (unstable) response. This is usually a study, planning function, but may be making its way into the control room.

2. Tools Categories and Relationships

Used Off Line

- **Power System Model** (Model)
- **Network Reduction** (NR)
- **Eigenvalue Analysis** (EIG). Study planning function.

Used In Control Room

- **SCADA**

- **Power Flow (PF):** Base Case Starting Point for Security Analysis Functions

  - **Security Constrained Dispatch (SCD)** A form of OPF is used to calculate security constrained commands and selected contingencies.

  - **Optimal Power Flow (OPF) –** steady state operation: Solution core is often used for **SCD, VVD** (Voltage VAR Dispatch) and **SCOPF** (Security Constrained OPF)

  - **Static Contingency Analysis (SCA)**

  - **TSA (Transient Stability Analysis), MSA (Mid-Term Stability Analysis) and LSA (Long-Term Stability Analysis)** compute the reaction to contingent conditions. Explore many pre-specified contingencies (considered potentially harmful) that come out of fast screening techniques.

3. Independent Observations and Comments on the ISA Tools

Following are summary comments on the tools based on the results of the survey.

- **VVD, MSA, LSA and EIG** are all either rarely used or not useful.

- **TSA** is very important to several organizations, but it is very time consuming. In addition, there are just a few “trial and error” approaches for this analysis. There is no "bible" analysis approach; therefore it is rarely used for practical systems. Creating and maintaining data models is a problem.

- **OPF** is useful but not used very often. Maintaining accurate information is an issue.

- **SCD and SCOPF** are rarely used. They are complex tools and time consuming to set up and maintain (again a data modeling issue).

4. Survey Results – "High Level" Summary and Overview

ISA Tool	Parameter of Interest	Data and Notes
Model	Effectiveness/Robustness	Satisfaction varied considerably.
	Data exchange	Y (10), N (9)
	Exchange format	Various vendor formats in use.
	Exchange freq	1 to 90 days
	Size	As large as 10K subs, 14K buses, 16K lines, 3K gens
NR	Performed	Off-line
	Frequency	2 months to 1year.
SCADA	Status	All operational
	Effectiveness/Robustness	Mostly satisfied
PF	Performed	On-line
	Status	All Operational
SE	Effectiveness/Robustness	All but 2 quite satisfied
	Status	All operational.
	Performed	On-line
	Update Frequency	1 to 10 minutes
SCA	Status	Operational
	Performed	On-line
	Execution Time	2 to 200 sec
	Update Frequency	1 to 30 min
SCD	Status	Most unavailable or not used.
OPF	Status	Only 4 operational.
	Performed	Both on-line and off-line.
	Execution Time	90 to 200 sec
	Update Frequency	1 week (for 1 company).
SCOPF	Status	Only 1 operational.
VVD	Status	Most unavailable or not used.
TSA	Status	6 operational.
	Performed	Most off-line.
	Execution Time	Time consuming: 4 min to several hours.

ISA Tool	Parameter of Interest	Data and Notes
MSA	Status	Unavailable or not used.
LSA	Status	Unavailable or not used.
EIG	Status	Unavailable or not used

5. Synthesis of Survey Information

The key questions to be answered fall into five categories as shown below. Survey results were grouped according to the questions.

1. **Use of the Tool**: Is a tool being used? Which tool or tools are actually being used and pursued?
2. **Effectiveness and Robustness of the Tool**: What works? What does not work?
3. **Gaps in the Tool**: What's missing (where are the gaps)? What gaps are repeated?
4. **Trends**: What are the trends?
5. **Wants:** What do operators need that they do not currently have?

- Reported details of the number of buses, nodes and lines in a particular system model, for example are not shown in the following tables to protect potentially sensitive information. Also, analog inputs, scan rates and so on for the SCADA tool, as implemented by a particular responder, are not shown in the following tables. The size of a particular system model run by a particular tool, for example, may be important in some cases. It can bear directly on the cost of maintaining the model and, consequently, on the willingness of that particular company or organization to invest in the necessary maintenance resources to enable the company or organization to reap the maximum benefits of running the model.

- For the most part the comments have been rephrased and reorganized as needed to fit the various question categories. For example, a comment that includes a description of a number of problems or gaps has been rephrased to show the problems or gaps in point form.

- The term “Tool not specified” is used to indicate that within the interviewer notes the actual software package that the responder is using was not specified. However, the use of the term within “Tool Used” means that the tool is being used.

Power System Model

Acronym	**Model**
Tool Used	All organizations have a model building and maintenance tool.
What Works	Internal models are generally well maintained.
What Does Not Work	• Buffer and equivalent areas of the model are often problematic. • Exchange with other organizations is not generally a smooth process. • The topology is often problematic because disconnects are open while breakers are closed. • Bringing updated models on-line should be done more frequently (and easily). • A big issue is the uncertainty of generator data outside of a utility's system. • Work flow management in the enterprise from planning through construction and maintenance is a problem. • Tools for import/export must deal with different vendor formats and translations often lose information. • Exchanging model information can have significant political problems. • Manpower for modeling is the worst area.
Problems and Gaps	• Weakness is getting data from neighbors. Worried about security information. Had to add internal tools to help create and maintain the model. Controls in the system are linked, but modeling tools in the product do not reflect the field. Control models need to be enhanced (universal controller model) to fix this. Little patches aren't so good. Better to model what's really in the system and not have to create work arounds. • Changes all done manually. Looking at CIM XML exchange. Big issue has to do with keeping the far away places up to date. • Biggest problem is maintaining the system model. • Getting CIM XML, model exchange and merge. • Capability exists to provide CIM XML per NERC requirements; however import of data into EMS in that format is not currently available or anticipated in the short term. • Special model for entities like combined cycle units, generation dependent station service and so on, where the relationship among devices is considered, could use improvement. • Current tools in EMS's tend to be statically sized such that resizing historically generated cases are not backwards compatible.
Repeated Gaps	
Wants	• Tools to electronically move models with CIM XML would be great. • Tools to help with modeling, creating externals and network reduction. • Would want to use other security assessment tools if they had their models in order.

Acronym	Model
	• Would like to get accurate data. Moving data through the ISO system (from member to ISO) does not work well. The ISO does not own the assets and the owners do not always provide accurate information. Better processes and engineering resources are needed. An exchange format (CIM XML) will help this. If member organizations can adopt such an exchange then it may clear things up. In general, improve the process. • Display building tool that updates the data base from the display. Do not believe in auto generation of displays. • Automated one line building. Done by hand now. • Partial/incremental update capability. • Standard naming convention to use CIM XML effectively. NERC is making slow progress. Automatic identification of ICCP ID is just now being addressed in model exchange format work. • Auto display generation tool from the native model. Substation basis is fine. Must be able to take high level guidance from display builder on a substation basis or create substation templates to apply to substations with similar layout needs. • Automatic linkage to application data. Currently very error prone. • ICCP bi-lateral tables need to be automatically generated for internal use. • Dynamic sizing of models.
Trends	• Modeling is the biggest area of interest. • Plan to use CIM XML exchange format in future. • “Graphical” maintenance tools may be considered if it is proven to improve maintenance efforts over that offered by existing tools.

Network Reduction

Acronym	NR
Tool Used	• Operations model uses the NERC MMWG case_which has already been equivalenced using PSSE. • Do not do data reduction. • Rigid model produced. Putting a generator and load out there seems to work just as well. Comes from network planning. Updated only when you know something from the neighbors. • Model created from NERC Multiregional Modeling Group (MMWG) power flow information. • Do not do reduction. • Equivalents are manually put into the operational model, based on results of NR tool. • Equivalents are in the model but have not been updated.
What Works	• Often external information is retained and not reduced.

Acronym	NR
What Does Not Work	• Exchange of information with neighbors to equivalize. • Time to create confidence with an equivalent
Problems and Gaps	• Data submitted by each MMWG company varies in detail and modeling techniques. For example, some utilities model generators in detail while other utilities model generators connected to a bus as a single generator with no step up bank whose generation value is the sum of the generators at that bus. • Problem with external modeling is the effort (lack of tools) to efficiently modify/replace external models that are in the EMS DB model. • Need better NR tools to allow for accurate system equivalence on real time basis.
Trends	• Efforts underway to automate the process of efficiently modify/replace external models that are in the EMS DB model. Goal is to be able to quickly change portions or all of the external models to take advantage of data exchange values or special modeling needs.

Supervisory Control and Data Acquisition

Acronym	SCADA
Tool Used	• All organizations use SCADA.
What Works	• Very satisfied.
What Does Not Work	
Problems and Gaps	• Too many alarms but is a configuration issue they have under control. • Sometimes lose large “chunks” of data from regional centers that cause SE and holes in the SCADA. Old indication is made but that happens rarely. Achieving something higher is probably not worth the effort. Concerned that with system blackout this may be a problem but it has not been a problem so far. • Unstable data is the biggest problem. Data come from 20 utilities and therefore there is a lot of data conversion required.
Repeated Gaps	
Wants	• More intelligent alarming that points out the worst situations and pinpoints the problem from all of the alarms. May not be currently taking advantage of the vendor supplied tools to do this.
Trends	• Plan to add status estimator. This is deemed important as most state estimators take the status information as “gospel”. Want to increase ICCP analog updates to 60 seconds from 120. Status currently comes by exception.

Power Flow

Acronym	**PF**
Tool Used	• All organizations use a power flow tool.
What Works	• Works good.
What Does Not Work	
Problems and Gaps	• Issues with the load model – P versus I versus Z. Power factor is often unknown because of capacitor switching. • Usability is poor. • Support staff runs the model for operators. • Only 10 copies available for users. • Only a certain number of output displays for many different applications. • Complexity of navigation on the application control display. • Creating displays is very hard and involves code. • General maintenance is a problem with this architecture. • Case set up is very hard. • In general the security tools are difficult for the operators to use. They require a lot of "care and feeding". Need to work reliably or credibility will be lost. • Switch status may be wrong from state estimator. • Biggest issue is changing the load model when they predict dramatic load changes and transfers. • The state estimator (SE) fed power flow sometimes cannot solve if there is a "big smash" on the system
Repeated Gaps	
Wants	• Auto display generation would help. • Need to work reliably or credibility will be lost.
Trends	

State Estimation

Acronym	**SE**
Tool Used	All organizations running a state estimator.
What Works	• Very happy • Works satisfactorily. • Works great.
What Does Not Work	• Bad data part is turned off. Needs work.
Problems and Gaps	• Frequent observability problems. • Need modeling flexibility to put measurement where it exists.

Acronym	SE
	• Parameter estimation and abnormality detection are not done well. Hard to change. • Series capacitor status seems to have a lot of bad data. • Switch position is not being estimated. Skeptical that this can be done properly. Believe that the best solution is to get switch position monitored and updated properly. • Biggest issue is no detection of possible status measurement problems. Assumes all of these are correct. • Bad data part is turned off. Needs work. • SE will not converge with "big smashes" on the system. This can last for 10 minutes or an hour. Sometimes it needs a model correction. • Some information is manually maintained. This can "throw the solution off". Often this is in poorly measured areas with no redundant information. • Topology error detection that may fall below the level of mismatch tolerance of the model. • Run bad data first then correct problems. Turn off bad data analysis when they run SE. • Have to estimate IPP outputs (measurement problem). • Status is taken as "gospel". • Observability is poor and data communication needs more attention.
Repeated Gaps	• Uncertainty about the status of switches in the system.
Wants	• Data links to have a full measurement observable system with the entire interconnected system from 230 kV on up. • Estimation or error detection that alerted operator to inconsistent status information. Needs to run as fast as SE. • A "bad topology" identification algorithm would be beneficial. • Would like to see anomaly detection reporting and comparisons with SCADA values done better. There are tools in the product to do this but some organizations use their own tools to download and compare the data and then follow-up on what may be causing problems. Having this flexibility (facilitating the use of scripts) allows the user to be in control of things that have personal preferences.
Trends	• Bad error detection and status detection becoming more common.

Static Contingency Analysis

Acronym	SCA
Tool Used	• Most sites used contingency analysis. • The analysis uses linear (but operating point dependent) methods with full power flow available on demand." • Use full Newton power flow for contingencies.

Acronym	**SCA**
	• Thermal contingencies aren’t as important as stability limits. • They are concerned about short circuit currents when switching lines in. Planning has set maximum fault currents based on duty capabilities of the breakers. Since planning has considered all units on, the guidelines are considered conservative. Using these guidelines would prevent switching at times. The operators have created their own program to utilize short circuit calculations with actual duty capabilities. • Could run this more often than every 5 minutes. This runs after State Estimation (SE). • The contingency analysis is run every third State Estimation solution. • Security Analysis package solves 2000 full power flow contingencies in one minute. Provides thermal and voltage drop limits. Have power flow for voltage stability analysis to compute transfer limits across predefined interfaces. This takes 3 minutes. • Have off-line contingency analysis program (internally developed). Handles 2700 contingencies (full N-1 on lines and transformers). Runs in 60 s. • Have off-line full N-1 solution (with steady state stability) to supplement EMS execution. • 50 contingencies are related to flowgate monitoring and security. They are interested in this overview because they have oversight. The other companies are looking at the myriad of contingencies in detail.”
What Works	• Happy with the tool. “Only one contingency is forced to full PF. Others may go to full PF on a dynamic basis as determined by the software. Speed of solution is not an issue. • Solves fine.
What Does Not Work	•
Problems and Gaps	• The contingencies give overloads that are not real. • Constraints and limits are not modeled as well as they need to be for this to be used. • Cumbersome for control room use. • Maintenance intensive – with reference to keeping up to date. • Only good if SE is good. • Only looks at thermal issues. • Recognizing voltage sag problems caused by transfers can be an issue. • Some contingencies are modeled without a special protection system (specially designed automatic control for a specific contingency). These SPS’s are sufficiently complex such that the tool cannot represent them. The operator must then figure out whether the contingency is a real problem or one that an SPS could solve. This is a particularly significant problem for ISOs and RTOs. • At the time of the interview the dispatchers were in the process of setting up the contingency lists. It appears that the process was slow because

Acronym	SCA
	the dispatchers did not see the need for the lists. New staff member required at this organization to set up the data bases, maintain the data bases and carry out the analyses with the tool. Need to define what is screened and what is fully processed. • Ability to manage and present the large quantity of results so that an operator can understand what they are seeing. • Tool has some coding errors that result in the base case moving slightly as each contingency is processed. The next version of the tool is supposed to fix this. • Currently get a long list of information from the tool that is hard for the operator to process. The operators have scripts that look for contingencies for the flow gates to see if they are getting close to their ratings. With scripts they can be in control of exactly the information that they want. This important flexibility may be better served with scripts than building it into the tool itself.
Repeated Gaps	• Output is difficult for operators to process.
Wants	• Needs to predict arming of generation shedding under contingencies. • Need to model RAS. • Good angle difference measure. • Could SCA be modified to handle transfer levels as contingencies to warn operators of what could happen? • List contingencies in a reasonable priority fashion. • Operators would like to have the distribution factors available should a problem occur. Currently they are hidden. • Ability to manage and present the large quantity of results so that an operator can understand what they are seeing. More work needs to be done in the areas of contingency analysis results presentation and alarming. • Better post processing of the contingency list.
Trends	

Security Constrained Dispatch

Acronym	SCD
Tool Used	• Have a tool but it is not used. • Do this on an operations planning basis. • Available in an “open-loop environment”, but not used. “ • No plans to use this. • Interesting, but needs to maintain a more accurate model first.
What Works	•
What Does Not Work	•

Acronym	**SCD**
Problems and Gaps	• Support staff needs to get accurate data from neighbors to make this worthwhile and work right. The issue is how to get reasonable up to date information from groups that don't report to you? • Complexity of the problem leads to complex user interfaces as well as making it hard to validate.
Repeated Gaps	•
Wants	• The biggest need obtaining realistic solutions an operator would perform and not just an answer (i.e. he won't move 25 controls a little when he can move 3 a lot and achieve nearly the same response." • Automatic consideration of all possible "switching scenarios" as controls rather than having to define a predefined set which may or may not include the optimal control.
Trends	

Optimal Power Flow

Acronym	**OPF**
Tool Used	• OPF is run in study mode with real-time data on an as needed basis. . • Used once per week on average when there are problems with a flowgate approaching its limit. • Available but not used. • It's all scheduled, no real need. • Do not have an OPF. • Not worth the effort to use it.
What Works	•
What Does Not Work	• The delivered product was useless. Very confusing. Use died.
Problems and Gaps	• The vendor-supplied OPF only has traditional objective functions such as minimize losses. They are not interested in this. • Not worth the effort to use it. • Using the tool to cover all the different operating scenarios is difficult". It takes a lot of time. It can be dealt with better using operating experience and engineering judgment. • Requires good models and keeping them up to date. • Too finicky. The reactive side of the situation seems to be very hard to get right, especially with the rough load models." • The only good study would be to store historical data that depicts (sic) the situation of interest. • Lack of funding to use the tool. • Difficult to control re-dispatch after a unit outage. There appear to be ways to do this with the tool, but they are not easy or intuitive.

Acronym	**OPF**
	- Training is an issue
Repeated Gaps	-
Wants	- Would like to reduce losses. An OPF could help with this. However, there are not a lot of controls on their system. - Want an OPF, however maintaining the system model is their biggest problem. That needs to be addressed before they move on to use tools like OPF. - Better load modeling, especially modeling of load power factors and reactive power.
Trends	

Security Constrained Optimal Power Flow

Acronym	**SCOPF**
Tool Used	- Generally either not available or not used. Off-line studies generally used for this type of information. - They take the output from their Security Analysis tools and send them into their Unit Dispatch System (both 20 minutes ahead, and real time). The Security Analysis tools give suggestions for eliminating violations. These suggestions are used in the Unit Dispatch System to eventually eliminate violations. - Would like to have an SCOPF. - Interesting, but need to maintain better, more accurate model first.
What Works	-
What Does Not Work	-
Problems and Gaps	-
Repeated Gaps	-
Wants	- Want SCOPF to advise how to set phase shifter taps to avoid insecure cases during contingencies.
Trends	

Voltage VAR Dispatch

Acronym	**VVD**
Tool Used	- Most analysis is done off-line. - They perform voltage collapse studies occasionally although this is not

Acronym	**VVD**
	an online function done routinely. They use a 500MW margin to back off from the nose curve maximum. They monitor reactive power reserves and voltages at critical buses. • This type of study is done seasonally. • There is no systematic procedure. The schedule is given by planning to the plants for day, night and weekend. • They had a voltage scheduler, but it was not used. They would like something. • They are doing some work heuristically today…rules that they follow. • Interesting, but need to maintain model first • This is available in an open-loop environment, but is not used. • Voltage issues are not a concern.
What Works	•
What Does Not Work	•
Problems and Gaps	• An integrated package for voltage and transient stability would be very helpful. Problem in getting consistent results that don't recommend changes that disrupt another area.
Repeated Gaps	•
Wants	• They had a voltage scheduler, but it was not used. They would like something. • They would like to have such a tool that does some very simple things. E.g., if control voltage at a bus, which controls could you use (simple sensitivities). • An integrated package for voltage and transient stability would be very helpful for them." • Better integration of all these ISA tools is needed with better maintenance and less complexity. Get data to flow smoothly between applications." • An integrated package for Monitoring VAR reserves, but don't see a need for this tool.
Trends	

Transient Stability Analysis

Acronym	**TSA**
Tool Used	• Planning does all of this. • Table based tool from studies off-line with a sophisticated rule based selection capability. Recommends shedding schemes every 4 minutes. It has automatic shedding routines for arming the RAS. Also recommends the operator to take action (generation distribution, etc.).

Acronym	TSA
	• Use a voltage stability tool that calculates the percentage of a line removed. Varient of a QV. The new replacement is a PV. This is very unique. • Off-line studies go into transmission operating guides. These studies continue to go on with operating guides being updated. All lines in, single element out screened. They do manual sensitivity analysis to try and see important correlations.
What Works	
What Does Not Work	
Problems and Gaps	• Labor intensive. • Execution time. • Not well supported, so it is not used now.” • TEF method cannot screen complicated faults (misoperated relay, breaker failure, HVDC reduction, etc.). • They think that they have the problem of extra data fixed as they have a bridge between their EMS data and the DSA requirements.
Repeated Gaps	
Wants	• On-line tool. • Testing of the recommendations would be very helpful to reduce the time to do this. • It would help the new engineers to have tools that help understand the sensitivities and direct the studies. • Might be good to have an on-line tool that does this, but there is skepticism, mainly with the pain to be endured to get it to work right.” • Biggest upcoming need is the availability of a transient stability tool for the operations environment (with high performance contingency evaluation and a user interface that does not require the operator to look through a lot of data).”
Trends	

Mid-Term Stability Analysis

Acronym	MSA
Tool Used	• Planning does this. • The planning department does this. They set operating limits on corridor flows and voltages.
What Works	
What Does Not Work	
Problems	

and Gaps	
Repeated Gaps	
Wants	• This would be nice to have, but low on priority list.
Trends	

Long-Term Stability Analysis

Acronym	**LSA**
Tool Used	• Planning does this. • Voltage stability is studied off-line. • They have long term oscillation problems, but in general not worth the effort.
What Works	
What Does Not Work	
Problems and Gaps	
Repeated Gaps	
Wants	• This would be nice to have but low on priority list.
Trends	

Eigenvalue Analysis

Acronym	**EIG**
Model Used	• Planning does this. • Sometimes in planning. • OK in system planning, but not in operations planning. They have an eigenvalue tool for planning, but try to use transient stability in operations planning."
What Works	
What Does Not Work	
Problems and Gaps	
Repeated Gaps	
Wants	• Would like to shift from transient stability to eigenvalue analysis without a lot of set up. Then it might be helpful in an operational sense. • Would be nice to have, but low on priority list.
Trends	

7. Glossary

(See definitions in section 1. for additional acronyms)

CIM Common Information Model

CIM/XML Computer language that is used to represent power system models. The CIM/XML language introduces a power system oriented vocabulary that includes “transformer” and “breaker”. These vocabulary items are drawn from the CIM schema. It has been adopted by the utility industry body NERC as the standard for exchanging models between system operators.

EMS Energy Management System

ICCP Inter Control Center Protocol

ISO Independent System Operator

IOU Investor Owned Utility

MMWG NERC Multiregional Modeling Working Group

NERC North American Electric Reliability Council

RAS Remedial Action Scheme

RTO Regional Transmission Organization

XML eXtensible Markup Language. Technology for encoding structured documents in new applications. XML is a markup language developed by the World Wide Web Consortium (W3C) and standardized by a W3C recommendation. It is now the format of choice for document-level data exchange over the public Internet and within many private networks. Two of its antecedents are the Standard Generalized Markup Language (SGML) and Hypertext Markup Language (HTML). XML is generic.